REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	12 May 1996	SSC Fellow Research Paper

4. TITLE AND SUBTITLE

Grand Strategy for Information Age National Security

5. FUNDING NUMBERS

6. AUTHOR(S)

KENNEDY, KEVIN J., LtCol, USAF
LAWLOR, BRUCE M., COL, USARNG
NELSON, ARNE J., CAPT, USN

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

US Army War College
Root Hall, Bldg 122
Carlisle Barracks
Carlisle, PA 17013-5050

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Harvard University
JFK School of Government
79 JFK Street
Cambridge, MA 02138

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

Current national security strategy is obsolete. Based upon industrial age threats and defenses with limited information-age applicability, it fails to defend against structured information attacks threatening US centers of gravity, and relies upon DoD as sole provider of national defense in the information dimension.

US technology dependence presents a strategic threat to the information systems that control key aspects of our national power. Future competitors may undermine our national will to fight by exploiting our reliance upon information systems, our present technological vulnerability. This threat would be most effective in situations where US forces application is discretionary, and the desirability of employment is not obvious.

The study proposes a strategic framework demonstrating the potential strategic effects of information weapons employment and conceptualizing both offensive and defensive information campaigns, highlighting shortfalls in present policies by suggesting accessibility of US centers

14. SUBJECT TERMS			15. NUMBER OF PAGES
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

GENERAL INSTRUCTIONS FOR COMPLETING SF 298

The Report Documentation Page (RDP) is used in announcing and cataloging reports. It is important that this information be consistent with the rest of the report, particularly the cover and title page. Instructions for filling in each block of the form follow. It is important to ***stay within the lines*** to meet ***optical scanning requirements***.

Block 1. Agency Use Only *(Leave blank)*.

Block 2. Report Date. Full publication date including day, month, and year, if available (e.g. 1 Jan 88). Must cite at least the year.

Block 3. Type of Report and Dates Covered. State whether report is interim, final, etc. If applicable, enter inclusive report dates (e.g. 10 Jun 87 - 30 Jun 88).

Block 4. Title and Subtitle. A title is taken from the part of the report that provides the most meaningful and complete information. When a report is prepared in more than one volume, repeat the primary title, add volume number, and include subtitle for the specific volume. On classified documents enter the title classification in parentheses.

Block 5. Funding Numbers. To include contract and grant numbers; may include program element number(s), project number(s), task number(s), and work unit number(s). Use the following labels:

C	- Contract	**PR**	- Project
G	- Grant	**TA**	- Task
PE	- Program Element	**WU**	- Work Unit Accession No.

Block 6. Author(s). Name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. If editor or compiler, this should follow the name(s).

Block 7. Performing Organization Name(s) and Address(es). Self-explanatory.

Block 8. Performing Organization Report Number. Enter the unique alphanumeric report number(s) assigned by the organization performing the report.

Block 9. Sponsoring/Monitoring Agency Name(s) and Address(es). Self-explanatory.

Block 10. Sponsoring/Monitoring Agency Report Number. *(If known)*

Block 11. Supplementary Notes. Enter information not included elsewhere such as: Prepared in cooperation with...; Trans. of...; To be published in.... When a report is revised, include a statement whether the new report supersedes or supplements the older report.

Block 12a. Distribution/Availability Statement. Denotes public availability or limitations. Cite any availability to the public. Enter additional limitations or special markings in all capitals (e.g. NOFORN, REL, ITAR).

- **DOD** - See DoDD 5230.24, "Distribution Statements on Technical Documents."
- **DOE** - See authorities.
- **NASA** - See Handbook NHB 2200.2.
- **NTIS** - Leave blank.

Block 12b. Distribution Code.

- **DOD** - Leave blank.
- **DOE** - Enter DOE distribution categories from the Standard Distribution for Unclassified Scientific and Technical Reports.
- **NASA** - Leave blank.
- **NTIS** - Leave blank.

Block 13. Abstract. Include a brief *(Maximum 200 words)* factual summary of the most significant information contained in the report.

Block 14. Subject Terms. Keywords or phrases identifying major subjects in the report.

Block 15. Number of Pages. Enter the total number of pages.

Block 16. Price Code. Enter appropriate price code *(NTIS only)*.

Blocks 17. - 19. Security Classifications. Self-explanatory. Enter U.S. Security Classification in accordance with U.S. Security Regulations (i.e., UNCLASSIFIED). If form contains classified information, stamp classification on the top and bottom of the page.

Block 20. Limitation of Abstract. This block must be completed to assign a limitation to the abstract. Enter either UL (unlimited) or SAR (same as report). An entry in this block is necessary if the abstract is to be limited. If blank, the abstract is assumed to be unlimited.

★U.S.GPO:1991-0-305-776

13 ABSTRACT (cont.)

of gravity and limitations of protecting against employment of information weapons. It recommends that certain information systems, as strategic national security assets, require protection and demonstrates how strategic warfare's scope expands into the broader information dimension of conflict.

Information assurance should be the theme for US defensive grand strategy, giving priority to the systems most essential to our national information infrastructure and systems that permit command and control and employment of military forces. A strategic plan for information assurance is offered.

GRAND STRATEGY FOR INFORMATION AGE NATIONAL SECURITY

"Information Assurance for the 21st Century:

A National Commitment
that secures confidentiality, integrity and availability of our information and reliability of our information systems;

A National Consensus
balancing government security and personal protection with
US Constitutional guarantees and American notions of individual liberties."

Lt Col Kevin J. Kennedy, USAF
COL Bruce M. Lawlor, USARNG
CAPT Arne J. Nelson, USN

Harvard University
John F. Kennedy School of Government
National Security Program
Policy Analysis Paper
Final Draft

About the Authors

The authors were National Security Fellows at Harvard University, Kennedy School of Government during the 1995-96 academic year, when they researched and wrote this paper.

Colonel (sel) Kevin J. Kennedy, USAF, a command pilot, most recently commanded a Primary Jet Flying Training Squadron in Air Education and Training Command. His previous flying assignments include duty as an operations officer of a B-52 Bombardment Squadron, chief of Wing Safety in the B-52/KC-135 Training Wing, chief of Training in a B-52 Squadron and as a T-37 instructor pilot. He has over 3200 flight hours. His staff assignments include Chief, Joint Strategic Planning Staff Briefing Branch, B-1B/B-52 strategic employment planner at Strategic Air Command Headquarters, and as an Air Staff Training officer at the Pentagon. Colonel Kennedy is a graduate of the United States Air Force Academy and holds master's degrees in National Security and Strategic Studies from the Naval War College and Human Relations from Central Michigan University.

Colonel Bruce M. Lawlor, USARNG, is a National Guard officer who has commanded the 86th Armor Brigade and the 1-172 Armor Battalion, Vermont Army National Guard. He has served as an executive officer, staff officer and commander at all levels in an armor brigade. He holds a Bachelor of Science in Political Science and Juris Doctor from the George Washington University. Colonel Lawlor is currently pursuing a Master of Arts in National Security Studies from Norwich University. He is a practicing attorney with national board certification in civil litigation and holds advocate status from the National College of Advocacy.

Captain Arne J. Nelson, USN, a Naval Aviator, commanded Helicopter Combat Support Squadron Four, homeported in Italy, during Operations Desert Shield and Storm, Provide Comfort in Northern Iraq and Sharp Edge in Liberia. With over 3500 flight hours, 3200 in H-53 helicopters, his extensive operational experience involved flying tours in Helicopter Combat Support and Helicopter Mine Countermeasures squadrons, and included fleet replacement squadron instructor duty. A qualified Joint Staff Officer, he served as Executive Assistant to the USACOM Director for Operations. Captain Nelson is a graduate of the University of New Mexico and the Armed Forces Staff College, and holds a master of science from the University of Southern California and a master of arts from the Naval War College.

Table of Contents

List of Figures

Executive Summary

New Strategic Threat

The information age brings enormous benefit to the United States, however, US dependence upon technology results in a new strategic threat aimed at the information systems that control key aspects of our military, economic, and political power. This factor, plus overwhelming US conventional military might, suggests future competitors may embrace grand strategies that avoid directly attacking US defense forces and focus on undermining our national will to fight by exploiting our reliance upon information systems, our present technological vulnerability, and our democratic method of governing. This threat would be most effective in situations where US force application is discretionary, and the desirability of its employment is not clear cut. Though it will never equate to the strategic threat of physical occupation by conventional military forces, it is a potent coercive policy weapon.

We believe the current US grand strategy for national security is obsolete because:

- It is based upon industrial age threats and defenses that have limited information age applicability.
- It fails to defend against structured information attacks threatening US centers of gravity.
- It is still reliant upon DoD as sole provider of national defense.

New Information Age Realities

Six information age realities produce a significant change to the national security environment.

Information technologies have created a fifth dimension of conflict. Recognizing the uniqueness of this dimension highlights the limited relevance of the world's most powerful army, navy, and air force in defending strategic centers of strength from information attacks. The sum of their conventional forces is far more potent than any would challenge conventionally, but are an inadequate deterrent to deflect information weapons or protect information targets.

In this new dimension, the ***rapid exploitation of information can produce significant advantages in warfare and in commercial competition.*** Leaders who exploit information technology may seize the initiative, get inside an opponent's decision making cycle, and thereby limit or channel the options available to it.

Moreover, in the information age interconnectivity and dispersed computing power have greatly expanded access and dependence upon information making the places it resides (data bases, communication networks, logic programs) more susceptible and attractive targets. Therefore, ***information itself must be protected.*** Information can be used as a weapon to corrupt or destroy, or it can be the target of an attack.

For as long as defensive countermeasures lag behind innovative use of offensive information weapons, the US will have ***new strategic vulnerabilities that make traditional notions of US physical sanctuary less meaningful***. Heavy US dependence upon information systems combined with today's worldwide interconnectivity of computer systems, that have limited self-protection features, has created an avenue for attack of strategic assets. Financial institutions, public switch networks, power plants and other strategic centers of strength could be at risk from information attacks and military conventional forces can do very little to protect them.

Additionally, since the ante to enter information warfare is on a scale far below that for conventional warfare, ***potential attackers expand far beyond traditional nation-states***.

If the US is to effectively build and execute a new grand strategy for national security, efforts beyond the military must be employed and ***new strategic measures of effectiveness are needed to prioritize both these efforts in both the offensive and defensive categories.***

Priorities for Protection within US Strategic Centers of Gravity.

Our strategic framework divides US strategic centers of gravity into five categories: leaders, system essentials, infrastructure, population, and defense mechanism. Though the US defense establishment, is able to defend these centers of gravity against physical attack, it cannot protect them against the flow of hostile information from outside sources. Future conflicts may see the use of both conventional and information weapons against these centers.

These weapons may be divided into categories according to their functions: conventional ***physical destruction*** weapons that target the enemy's physical assets for destruction; ***corruption*** information weapons that control, compromise, corrupt or disable the operating software of targeted information networks and systems; and ***perception management*** information weapons that affect what an enemy's information systems portray as reality.

Juxtaposing these weapons functions with national centers of gravity produces a strategic framework (figure ES-1), displays the information dimension of conflict, demonstrates the potential strategic effects of weapons employment, and conceptualizes both offensive and defensive campaigns. It also highlights shortfalls in present national security policies by suggesting the breadth of future battlefields, the accessibility of US centers of gravity, and the

limitations of protecting against the employment of information weapons. It also provides a reference for decision makers who must set priorities regarding which information systems require protection as strategic national security assets. Finally, it demonstrates how the scope of strategic warfare expands beyond the traditional dimensions of the battlefield into the broader information dimension of conflict.

	Leaders Government	**System Essentials** Critical nodes of: Energy distribution, telecom systems, finance	**Infrastructure** Transportation, key production	**Population** Citizens	**Defense Mechanism** Military forces, LEAs
Destruction Physical Destruction	-Elimination or isolation of leadership -Slows decision making	-Denial of service -Ripple effects -Isolates	-Creation of bottlenecks -Inhibits concentration of forces -Isolates	-Demoralize -Loss of will to fight -Stiffens resistance	-Disarms -Uncovers other centers of gravity
Corruption Internal Operating Logic	-Produces unwise decisions -Loss of popular confidence -Isolation -Misperception of events	-Interruption/ denial of service -Loss of confidence	-Creates bottle-necks -Inhibits concentration of forces -Isolation	-Creates confusion -Loss of security -Diverts energy -Promotes anxiety	-Produces unwise decisions -Isolation of leaders -Misperception of events -Failure of weapons
Perception Management Behavior	-Produces favorable decisions			-Produces pressures/ demands on leaders -Creates divisions -Manipulate passions	-Misperception of events -Produces unwise decisions -Creates divisions
Ignore	-Deemphasize damage	-Hide extent of damage	-Minor or inconsequential damage	-Control panic - Perception management	-Protect intel sources

(Fig. ES-1) A weapons effects matrix for the strategic battlefield.

While assertions of a national disaster may be somewhat premature, open source anecdotal evidence suggests the US is already vulnerable to information attacks. The National Communications System labeled the threat to US public switch network system as a "serious concern" in 1993 and said it was worse in their 1996 update, noting "threats [are] outpacing our deterrents while vulnerabilities are outpacing the implementation of protection measures."[1]

Moreover, applying the framework to a recent RAND war game shows that the enemy

made a concerted effort to attack the information systems that control the US system essentials to produce secondary impacts upon the US population, and thereby create pressures on US leaders to alter their chosen course. The analysis underscores the ramifications of information conflict for the nation's leaders and that perception management is the common thread in information conflicts. The degree of skill demonstrated in handling these issues determines the ability of government leadership to maintain the fragile link between it and the people. Unless leaders can answer the people's questions satisfactorily, the danger exists that public pressure will force national security policy changes that may not be in the nation's best interest.

Other Complications: Authority, Responsibility, and Plurality

The threat to US information systems from corruption weapons is a clear and present danger that demands immediate attention. The pervasiveness of information technologies across the political, economic, military and social fabric of American life pose a difficult defense solution that is far beyond DoD authority and responsibility. In the pluralistic US society, firmly founded upon the concepts of division of authority and separation of powers, authority will most likely never be given to any one government agency. Pluralism offers tremendous advantages over single party executive agents to ensure a healthy public debate. A pluralistic approach will more likely produce a public consensus that balances the need for government security and personal protection with US Constitutional guarantees and American notions of individual liberty.

Conclusions

We need a new national security grand strategy that includes defending the nation's

information infrastructure with the objective to develop the capability to detect, deflect and defeat a structured information attack on the US. Our strategic framework suggests ***information assurance should be the theme for US defensive grand strategy***. The protection of the information and information systems that are critical to US strategic centers of gravity must become the catalyst for cooperation between government and civilian entities and the driving force behind the development of new national security policies. Information assurance provides the basis for a unified response to meet the strategic information threat.

Priority must be given to protecting information and information hardware that control the systems categorized as system essentials that offer the most lucrative information targets. In addition, within the strategic centers associated with government, i.e., leaders and the defense mechanism, the systems that permit command and control and employment of military forces must also be protected. We believe the balance of information and information systems should be left to the private and commercial sectors.

Leaders	System Essentials	Infrastructure	Population	Defense Mechanism
Command &Control Networks	**Telecommunications Electric power Gas/oil pipelines Federal Inter-bank transfers**	**Transportation dispatch systems**		**Communication networks Logs/Pers Databases Transport. Mgt. systems**

(Fig. ES-2) Priorities for protection.

Recommendation: A Strategic Plan for National Security

Vision: Information Assurance for the 21st Century

A national commitment that secures confidentiality, integrity and availability of information and the reliability of information systems. A national consensus balancing government security and personal protection with US Constitutional guarantees and American notions of individual liberties.

Mission: Plan, assess, coordinate and conduct activities to achieve information assurance:

- Identify and assess vulnerable information nodes within priority areas for protection.
- Identify and assess the strategic threat to US information and information systems.
- Develop proactive prevention and control measures that detect, deflect and defeat intrusions into, or structured information attacks upon, priority areas for protection.
- Develop the capability to execute those plans.
- Develop national institutions that build US government and private sector equities in information assurance.

Goals: National Imperatives

- Lead a vigorous public debate, that the information age presents security risks that are economic and political, and not solely military in nature.
- Unify a government/private sector response to protect the confidentiality, integrity, availability, and reliability of US information and information systems against the strategic information threat.
- Ensure information assurance priority for protection is given to the specific system essentials strategic centers of gravity. Abandon the idea of universal protection in favor of selective defense of government and private sector information and information systems deemed critical to national security.
- Establish a National Information Assurance Council (NIAC) to make national security policy recommendations to the President, aimed at bringing about our national security vision of information assurance.
- Establish an Information Assurance Center, patterned after the Center for Disease Control, and answerable to NIAC to perform surveillance, research, prevention and control, and infrastructure functions within the information assurance mission.
- Expand US National Security Emergency Response Preparedness (NSERP) planning to include physical protection for key network switching and control systems that manage areas within our strategic centers of gravity designated for priority protection.

- Encourage the President and Congress to support the National Security Telecommunications Advisory Council's (NSTAC) effort to establish a Security Center of Excellence and expand the NSTAC concept by creating similar committees in areas designated for priority protection.

Goals: DoD Imperatives

- SecDef submit information assurance and its information age strategic implications as part of the next National Security Strategy and direct CJCS to promulgate a new National Military Strategy that addresses the information assurance vision and its wartime subset of information dominance.

- Retitle the Assistant Secretary of Defense (ASD) for C3I as the ASD for Information and incorporate CONUS defense against information attacks.

- Recommend a change to the Unified Command Plan. Designate CONUS as an area of responsibility (AOR): task CINCSTRATCOM or CINCUSACOM with a CONUS defensive information warfare responsibility. Assume aggressive, quantitative modeling and simulation effort for defensive information warfare.

- Assemble a DoD organization for defense information assurance. Use core competencies already available within DoD to replicate the health taxonomy used for national information assurance.

- Direct CINCUSACOM to restructure the Key Asset Protection Program (KAPP) by: (1) Assessing key asset vulnerabilities to corruption information weapons as well as physical destruction weapons; (2) Adding system essential priority areas for protection to the Key Asset List; (3) Expand the KAPP evaluation and review board to incorporate experts from appropriate fields; (4) Expand planning and training to incorporate new Key Asset List physical protection requirements; (5) Thoroughly document all actions needed to address information vulnerabilities.

- Merge KAPP analysis with current vulnerability net assessments to identify the potential repercussions of a structured information attack upon system essential assets. Assume aggressive, quantitative modeling and simulation effort for defensive information warfare. Recommend higher levels of information assurance for national security.

- Direct CINCUSACOM to review operational plans for the Land Defense of CONUS to incorporate potential impacts resulting from information attacks and degradations to the information infrastructure.

1. United States, National Communication System, "An Assessment of the Risk to the Security of Public Networks," (Washington: National Communications System, Dec. 1995) ES-1.

Chapter 1: Grand Strategy Is More Than Military Strategy

The US Should Re-examine its Defensive Grand Strategy in the Information Age

The dawn of the information age suggests a re-examination of US defensive grand strategy.[a] This paper examines that issue, focusing on national security, not as the exclusive province of the Defense Department, but as the sum of political, economic, and military elements of national power and as the product of US national will.[1] Its purpose is to highlight the tenuous nature of current US national security policy, introduce information age realities pertinent for future policy development, propose a framework for conceptualizing defensive grand strategy, and recommend both a vision and strategic plan to enact it. The paper intentionally avoids service specific, operational, tactical, or technical discussions.

Overwhelming US conventional military might suggests future competitors are likely to embrace grand strategies that avoid attacking US defense forces directly and instead focus on undermining its national will to fight by exploiting its reliance upon information systems, its present technological vulnerability, and its democratic method of governing. This information strategic threat would be most effective in situations where US force application is discretionary and the desirability of its employment is not clear cut. It will never equate to a strategic threat of physical occupation by conventional military forces, but it is a potent coercive policy weapon.

---

[a] **A Definition of Grand Strategy.** Grand strategy is the art and science of developing and using the political and economic powers of a nation, together with its armed forces, during peace and war, to further national interests, priorities and policies. Grand strategy harnesses the elements of power for the entire nation and not just its military forces. Military strategy is a subset of grand strategy and is the art and science of employing the armed forces of a nation to secure grand strategy objectives by the application of force, or the threat of force. It does not define grand strategy but rather is defined by it. Thinking about grand strategy requires a different approach to conflict. It dictates a process of from the top down analysis, moving from the general to the specific. All strategists must first conceptualize the conflict as a whole, i.e., visualize the battlefield at the strategic level. Only then can consistent operational and tactical discussions begin.

Information Technology Changes the Focus of Grand Strategy from the Military to Other National Power Centers

Carl von Clausewitz reasoned that commitment to war emerges from the confluence of three centers of national power: the people, the military, and the government.[2] When these three centers of national power unify around a common purpose to be achieved by force of arms, an "interactive trinity" emerges that produces the national will to fight.

Clausewitz believed the most effective grand strategy to disrupt this "interactive trinity" and thereby gain victory was to defeat the enemy's military forces. He reasoned that such a defeat uncovered the enemy's other more vulnerable power centers and required it either to yield or face destruction of its leadership and people.[3] This precept has dominated much of western military thinking about grand strategy since Clausewitz's treatise, On War, was first published in 1832.

Today's information realm is a new and separate dimension of warfare, however, that provides other nation-states and non-state actors with direct access to US strategic centers of gravity and thereby generates a new and different national security environment. The nation's defense forces remain a viable deterrent to conventional military attack against the US population and its civilian political, economic and social infrastructures. However, at present, they are neither structured nor empowered to defend against national-level information attacks, or information attacks outside of the DoD infrastructure, therefore their ability to provide protection for these national power centers is problematic.[b] This development creates new strategic

---

b According to the Defense Science Board, there is no nationally coordinated capability to counter or detect a structured information attack, a problem that is made more difficult by the fact that many systems are not controlled by the Department of Defense. The Computer Security Act of 1987 limits DoD's ability to use its core expertise (e.g. National Security Agency) to help protect these systems and restricts it to protecting federal government systems that handle classified information. The Act also assigns the National Institute of Standards and Technology (NIST) responsibility for protecting federal unclassified but sensitive information. No one is responsible for protecting commercial, public and private systems upon which national viability depends. US Department of Defense,

opportunities for the world's next generation of aggressors and significant problems for those who will be charged with defending against them.

Against this backdrop, three factors must be considered. First, the United States has become the world's most "wired" country. It depends upon complex, interconnected information network control systems for such necessities as oil and gas pipelines, electric power grids, national transportation systems, banking and financial transactions, commercial exchanges, and a host of other perhaps less essential activities.[c] This interconnectivity provides enormous economic, societal and political advantages to the United States. However, it also makes these information control systems vulnerable to information weapons and therefore potentially inviting targets for US competitors.

Second, the defenses needed to protect the United States against information attacks are incomplete, making the world's most technologically advanced nation at the same time its most technologically vulnerable. Once adapted to military uses and coupled with organizational and doctrinal changes, information technology could significantly alter the battlefield equation[4]. Because of its advanced technology, the United States is poised to achieve such a breakthrough. However, capitalization on information technology elsewhere could provide strategic leverage to nations presently thought incapable of opposing the United States and enable them to emerge quickly from their military obscurity with significant, perhaps decisive, advantages in future

---

Information Architecture for the Battlefield, (Washington: Defense Science Board, 1994) 36.

[c] Michael Brown, an analyst with Science Applications International Corporation, postulates a hierarchy of information needs in which societies first use information, then come to rely upon it, and ultimately come to depend upon it. Once dependence occurs, the society begins to organize itself around information. He argues that in the case of the United States, such dependence creates vulnerabilities. Michael Brown, "Information Warfare and the Revolution in Military Affairs," Seminar on Intelligence, Command and Control, (Cambridge: Center for Information Policy Research, Harvard, 1995) 6.

conflicts. This will remain a possibility until such time as the United States has developed and fully implemented defensive countermeasures to information warfare. At present, defensive countermeasures are lagging behind available offensive systems.

Finally, the same technology that provides access to the American infrastructure also provides a variety of individual and group actors with unprecedented levels of direct contact with the US population and with US government officials. Such access promotes a healthy democracy. In the highly interconnected United States, public sentiment drives politicians to act, or to refrain from acting, as never before. Decision makers must deal with the media in shaping public opinion that sets the limits beyond which US policy must not go. Information technology now provides others, both hostile and friendly, with the means to affect directly how Americans perceive their government's policies, their societal norms, and their needs for self-protection.[d]

There is a Lack of Consensus Concerning the Threat

Arguments against this scenario center on three key issues: economic interdependence, infrastructure robustness and the lack of technical expertise on the part of potential adversaries to carry out a structured information attack. These issues, when coupled with the requirement for an adversary to have solid intelligence for target selection, lead many to dispute the immediacy or validity of the threat on the US infrastructure.[5]

Those who doubt the nation is at risk claim that to conduct a structured information

---

[d] The impact upon the US population of potential occupation by a foreign force has always weighed heavy upon US decision makers. Washington understood the vulnerability of the US population to British information warfare and both Grant and Lee were attuned to the vulnerability of their respective populations. The difference is that information technology provides competitors with the ability to impact the US population without occupation.

attack[e] on the US is virtually impossible, and that anything less (i.e., a focused, regional or tactical attack) would not yield success. Economic interdependence, they claim, discourages information warfare because the costs of attacking US targets, e.g., financial centers, outweighs any benefits gained. While nation-states may accept this premise, terrorists and other non-state actors will care little for economic interdependence, and the ability to initiate information attacks while remaining anonymous diminishes the effectiveness of retaliation as a deterrent. The assertion that potential competitors lack technical expertise is belied by the record. Significant intrusions are happening today and in some cases are state-sponsored (see appendix A). The vulnerabilities discussed within this paper are all based on capabilities demonstrated by actual incidents. The assumption made is that malevolent actors will eventually capitalize upon demonstrated capabilities and known vulnerabilities to mount a structured attack.

1. Colonel Arthur F. Lykke, Jr., lecture, US Army War College, Carlisle Barracks, PA, Jul. 1995.

2. Edward J. Villacres and Christopher Bassford, "Reclaiming the Clausewitzian Trinity," Parameters, 25.3 (Aug. 1995): 9-20.

3. Carl von Clausewitz, On War, ed and trans by Michael Howard and Peter Paret, (Princeton: Princeton UP, 1976) 90.

4. Andrew W. Marshall, "RMA Update," memorandum for the record, 2 May 1994.

5. Martin C. Libicki, What is Information Warfare?, (Washington: Institute for National Strategic Studies, National Defense University, Aug. 1995).

---

[e] According to Julie Ryan of Booz Allen, a strategic attack would be one that embodies an intention by an adversary to inflict overwhelming damage with a desired goal of 60 to 100% loss of capability over time. It requires the ability to purposefully target entities while coordinating time and location of attacks and inflicting certain specific levels of damage, and requires significant intelligence capability to include comprehensive understanding of target functionalities and processes the reliance placed on individual targets and cascading effects. It requires the ability to deliver the means of attack. The scale of the attack would be difficult to conduct covertly.

Chapter 2: The Nature of the Threat

> In information war, if an enemy's information or information systems are threatened to the point where national leadership must take action, then information warfare is underway.
>
> John Alger
> National Defense University

The Purpose of Warfare is to Overcome an Enemy's Will to Resist

Clausewitz believed that war is "an act of violence to compel our opponent to fulfill our will."[1] The objective of grand strategy, in his model, is to achieve that purpose by disrupting the enemy's "interactive trinity" through defeat of its military component.[2] This is the paradigm that drives most grand strategy planning. There are other potential models, however, in which grand strategy may be able to achieve its objective without disarming an opponent. The experience of the United States in Vietnam is an example of strategic defeat in the absence of corresponding military defeat. The US departure from Somalia is an illustration of strategic withdrawal in a situation short of war where the US possessed overwhelming military superiority. Both of these instances suggest that actions generating internal political pressures within the United States can produce strategic consequences. For political systems, such as the United States, information warfare has the potential to generate enormous pressures on leaders to alter national policies. Accordingly, US grand strategists must view information attacks on this country not in the context of their immediate damage but in terms of their impact on the body politic.[3] In this regard, they represent yet another means of trying to compel an opponent to fulfill one's will.

Information Provides an Alternative Means of Attacking the National Will

The objective of information attacks would be to gain strategic leverage over US decision

makers by generating political pressures within the US population to change national policies. Such attacks could provide a means by which adversaries could coerce US leaders to pursue policies more aligned with their ends and objectives and without using conventional military force.

The efficacy of information as a weapon against the US is predicated upon three factors: 1) vulnerable networked systems can be disrupted to launch a structured information attack, 2) malevolent actors will seek to take advantage of these vulnerabilities, and 3) the US population is able to generate political pressures that change national policy.

Anecdotal Evidence of Disrupted Networked Systems

Emerging anecdotal evidence continues to demonstrate the vulnerabilities of networked systems to significant disruptions through accidental or intentional input problems. For example, in 1991 there was a near total shutdown of telephone service in the Baltimore-Washington area as the result of a three bit coding error where a "d" was replaced by a "6" in one byte of a software upgrade. This simple error caused disruption of AT&T long distance service to millions of customers for over four hours.[4]

In another incident, on 17 September 1991, AT & T announced a power interruption had caused two public switches to fail. This failure forced the shutdown of major airports that rely on ground-based telephone lines for air traffic control communications in the New York, Boston and Washington Air Route Traffic Control Centers. The result was disruption of the civil aviation industry in these centers for days, that in turn caused flight delays across the nation.[5]

In addition to system failures and software glitches, there is anecdotal evidence concerning the malicious interference with information systems. A November 1988 virus (Morris worm),

placed on the internet by a college student, infected 6000 host computers in less than two hours and cost between $100,000 and $10 million to clean up, affecting network links between MIT, University of California, Sandia Labs, Lawrence Livermore Labs, Los Alamos National Research Laboratories, and others.[6] In another incident, a Christmas card message sent over BitNet, a global academic network, landed in 2,800 machines in 5 minutes, including IBM's internal network. It took only five hours for the benign virus to spread 500,000 infections worldwide, forcing IBM to take the network down for several hours to accomplish repairs.[7]

In the military arena, anecdotal evidence suggests the United States has already become a target for information attacks by groups intent on frustrating US national defense policies. Shortly after Iraq's invasion of Kuwait in 1990, various groups and actors launched a worldwide effort to penetrate various sensitive US government and military computers. Both Washington and NATO were targets. Dutch crackers penetrated host computers at Lawrence Livermore Laboratories, then branched out to access other systems across the US. They successfully penetrated US military computer systems at least 34 times between April 1990 and May 1991. Pentagon officials report these same individuals offered to disrupt the US military's deployment to the Middle East in return for payment from Saddam Hussein in the amount of $1 million. Saddam spurned the offer (see appendix A for additional examples of information attacks).[8] [9] [10]

The anecdotal evidence suggests both nation-state and non-state actors are already using the techniques of information conflict to launch limited, uncoordinated information attacks against the United States. These attacks are growing concern within the US government. In a report released in October 1994, the DoD's Defense Science Board found:

> ...the nation is under IW attack today by a spectrum of adversaries ranging from the teenage hacker to sophisticated, wide-ranging illegal entries into telecommunications networks and computer systems. This threat arises from terrorist-groups or nation-states, and is far more subtle and difficult to counter than the more unstructured and growing problem caused by hackers. A large structured attack with strategic intent against the US could be prepared and exercised under the guise of unstructured hacker activities...[such a strike] could cripple operational readiness and military effectiveness [by delaying troop deployments and misrouting cargo planes, trains and ships].[11]

Information attacks may be divided into structured and unstructured attacks. Unstructured attacks, sometimes referred to as class 1 and 2 attacks, are aimed at individuals and corporations. Structured attacks (class 3 conflicts) are aimed at nation states or societies, are more analogous to traditional warfare, and are the information equivalent of a major regional conflict or total war. There have been no reported instances of Class 3 attacks to date. Together these attacks include a range of information activities from malicious and potentially dangerous computer pranks, to criminal hacking activities, to terrorist acts of destruction, through malevolently shaping a nation's perceptions and opinions, to executing intensely lethal attacks employing advanced information-based weapons during interstate conflict.[12]

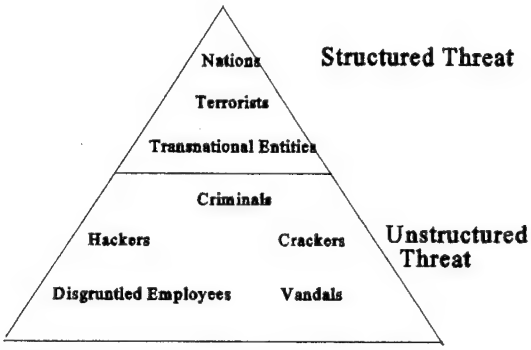


Fig. 2-1. The Structured and Unstructured threat.

Warfare is changing in the face of these threats and is adapting to them. We are witnessing the beginning of a new epoch in warfare that will supplement, and at times supplant,

lethal combat on the battlefield, and at its core lies information warfare.[13] Just as the airplane's adaptation to military uses led to fights to establish air superiority, the emergence of information as a strategic weapon will likewise lead to conflicts in which the first order of battle will be to establish information dominance over the enemy. Future conflicts may or may not be as lethal as those in the past, however, they are likely to witness mass upheavals in civilian populations. Increasingly frequent reports of computer crime and the potential of info-terrorism have heightened awareness of the nation's information vulnerability as opposed to vulnerability of physical assets.[14] As Winn Schwartau observed,

> The victims are not only the targeted computers, companies or economies, but the tens of millions of people who depend upon those information systems for their very survival. Take the power of class 1 and class 2 Information Warfare, multiply it tenfold, and you will begin to get a sense of the kind of damage that can be done. Class 3 information warfare creates chaos.[15]

The point of all this is not to suggest chaos on the information highway or that the United States is already locked in an information war with unidentified adversaries, but rather that offensive information capabilities already exist that can cause significant disruptions in the US population by attacking inadequately protected information systems.

Simulations Suggest Malevolent Actors Could Do the Same

Wargame simulations are also beginning to unmask the face of information conflicts and the problems associated with them. The RAND Corporation created and presented a game to senior government officials during 1995, entitled "The Day After...in Cyberspace."[16] The game's information incidents, for the most part, reflect actual examples of information system failures (see appendix B, figure B-2, RAND Wargame Incident Comparison). The game assumes the

incidents occurred as the result of actions by malevolent actors. The scenario postulates information attacks against the US and its allies in the year 2000 by a resurgent Iran. Officials playing the game were tasked, in the form of recommendations to the President, to formulate national security policies to counter this new form of warfare.

The enemy pursued three general objectives in the RAND game. First, it launched multiple and varied information attacks against numerous US and allied targets that were designed to generate internal political pressures and erode popular confidence in the ability of governments to control the developing crises. Second, it targeted allied infrastructure and military centers of gravity in an effort to disrupt the coalition's ability to fight. Third, it used conventional theater military operations to distract national decision makers from its information operations against the US. Figure 2-2 illustrates typical RAND targets and types of information attacks used against them (chapter 5 has an analysis of the RAND game; a full account of the game's highlights is in appendix B).

Transportation Systems	Sabotage of railway switches causes trains to slam together. Sabotage of commercial aircraft software causes planes to crash.
Tele-communications Systems	Disruption of public switching telecommunications networks in California, Oregon and Washington, and in Saudi Arabia, a US ally. Monitoring, interference, and theft of cellular subscription numbers.
Power Sources	Sabotage of a Saudi refinery computer results in an explosion and fire.
Financial Systems	Bank of England detects alien software designed to sabotage funds transfers. Software-induced ATM failures in Georgia banks cause run on other US banks. CNN reports Iran has hired hackers to attack western economies, resulting in US stock market plunge.
Military Forces	Disruption of phone service at key US military bases. Virus disruption of the Time Phase Force Deployment List (TPFDL) causes significant difficulties deploying US forces.
Political Systems	Special interest groups and other non-government organizations launch a significant propaganda campaign against the US population. Broadcasts of morphed political leaders of US allies made to sow discord among coalition members. Public demonstrations organized to undermine domestic and allied support for US national objectives.

(Fig. 2-2) Targets and types of information attacks.

The enemy's information attacks blurred the distinction between the requirements of domestic law enforcement and the greater demands of a national security crises. The players were ill-prepared for this new dimension of warfare and were unable to agree on what was happening or how to defend against it. Decisive recommendations were difficult to generate and traditional military responses to rapidly changing events and non-traditional attacks were not effective.

Game participants, who were mostly senior government and DoD officials, failed to reach consensus regarding the seriousness of the threat with their assessments ranging from "not a problem" to "couldn't be worse." The more time they spent on the problem, however, the more they considered it to be a difficult one that lacked concrete solutions and, in some cases, even starting points. In the end, most tended to describe the threat as one of greater magnitude than they had believed it to be before playing the game.

The Pentagon's Defense Science Board (DSB) has reported the existence of vulnerabilities in the US information infrastructure that mirror those highlighted in the RAND war game. Vulnerabilities listed by the DSB and exploited in the RAND game include perception management of events or circumstances, deception, manipulation of information content or delivery, and the debilitation or destruction of information.[17] Echoing RAND's game scenario, the DSB also stated that activities and capabilities already exist that give cause for concern over the integrity of information systems that are key enablers of military superiority.[18] It notes that although there are limited efforts underway to detect and counter unstructured threats to US information systems, there is no nationally coordinated capability to detect, much less counter, a structured information attack by a determined adversary.[19]

1. Clausewitz, 75.

2. Clausewitz, 89.

3. United States, National Communications System, The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document (Washington: National Communications System, 1994) 2-24.

4. Science Applications International Corporation (SAIC), Planning Considerations for Defensive Information Warfare - Information Assurance, (Washington: SAIC, 16 Dec. 1993) 36.

5. United States, Government Accounting Office, "Information Superhighway: An Overview of Technology Challenges," Report to the Congress, (Washington: GAO, 23 Jan. 1995) 37; also, Winn Schwartau, Information Warfare: Chaos on the Electronic Super Highway, (New York: Thunder's Mouth Press, 1993) 127.

6. Philip Elmer-DeWitt, "The Kid Put Us Out of Action," Time, 14 Nov. 1988: 76.

7. Lawrence J. Haas, "NII Security: The Federal Role," draft, (Washington: National Information Infrastructure Security Issues Forum, 14 Jun. 1995), 18.

8. Wayne Madsen, "Intelligence Agency Threats to Computer Security," International Journal of Intelligence and Counterintelligence, 6.4 (Winter 1993), 437-438.

9. Leonard Lee, The Day the Phones Stopped, (New York: Donald I. Fine, Inc., 1992).

10. Douglas Waller, "Onward Cyber Soldiers," Time 21 Aug. 1995: 44.

11. United States Dept. of Defense, 1994 Defense Science Board Summer Study on Information Architecture for the Battlefield, (Washington: Defense Science Board, 1994) 52.

12. Jeffrey Cooper, "Another View of Information Warfare: Conflict in the Information Age," draft, (Washington: SAIC, 30 Aug. 1995) 3.

13. Alvin and Heidi Toffler, War and Anti-War: Making Sense of Today's Growing Chaos, New York: Warner Books, 1993).

14. Cooper, 5.

15. Schwartau, 291.

16. RAND Corporation, "The Day After...In Cyberspace." (Santa Monica: RAND, 1995) 33.

17. United States, Dept. of Defense, Defense Science Board, 28, 51.

18. United States, Dept. of Defense, Defense Science Board, 51.

19. United States, Dept of Defense, Defense Science Board, 25.

Chapter 3: New National Security Realities

> The Commission considers the security of information systems and networks to be the major security challenge of this decade and possibly the next century...We have neither come to grips with the enormity of the problem nor devoted the resources necessary to understand fully, much less rise to the challenge.
> Joint Security Commission Report to SecDef and DCI - Feb 94

Dramatic Technological Changes Have Produced New National Security Realities

Revolutionary developments in information technology are producing a revolution in military affairs that changes the realities upon which United States grand strategy is based. The following information age realities contribute to the foundation for a new grand strategy. These new realities are ordered and build upon each other:

- ***Information technologies both modify the traditional spectrum of warfare and create a fifth dimension of conflict***. Revolutionary changes in warfare provide vast new opportunities with some liabilities - new strengths to be developed, new vulnerabilities to be protected, and new avenues to fulfill political ends.

- ***Rapid exploitation of information can produce significant advantages in warfare and commercial competition.*** Leaders who understand this new reality have the potential to get inside a competitor's decision making cycle, seize the initiative in combat or commercial competition and thereby gain advantages over an opponent.

- ***Information itself must be protected.*** Reliance upon information systems to enhance decision cycles can become a liability if corrupted or destroyed data produce bad decisions. The places where data and information reside (data bases, communication networks, logic programs) are alluring targets in a society heavily dependent upon them.

- As long as defensive countermeasures lag behind innovative uses of offensive information weapons, the US will have ***new strategic vulnerabilities that make traditional notions of US physical sanctuary less meaningful***. US dependence upon information systems, combined with today's worldwide interconnectivity of computers has created an avenue for attack of strategic assets. While financial institutions, public switch networks, and power plants remain relatively safe from crippling physical attacks, there is markedly less assurance that they are safe from information attacks because there are limited self-protection features in place.

- ***Actors other than traditional nation states can initiate information attacks***. Since the ante to enter information warfare is on a scale far below that of conventional warfare, potential attackers are not limited to traditional nation states.

- If the US is to effectively build and execute a new grand strategy for national security, ***new strategic measures of effectiveness are needed to prioritize both offensive and defensive efforts***.

These realities highlight the obsolescence of national security that plans a defensive grand strategy based solely upon conventional military forces. The Defense Department can no longer be the sole provider of national security. Defending information infrastructure, financial institutions, and other critical nodes from information attacks is beyond military authority and capability.[1]

Information Technologies Both Modify the Traditional Spectrum of Warfare and Create a Fifth Dimension of Conflict

> I think it's appropriate to call information operations the fifth dimension of warfare. Dominating this information spectrum is going to be critical to military success in the future.
>
> General Fogleman, CSAF

Information technologies have permanently modified the preexisting four dimensions (air, land, sea, space) of warfare. Desert Storm provided examples of this truth. Unparalleled information technologies produced greater weapon lethality and unprecedented clarity of the battlefield. The technologies that produced the lopsided victory continue to improve and are being driven not by military necessity but by commercial demand for improvements in information management.[2]

The nation's historic military leadership in technical development has ended. Commercial markets now influence deployment of advanced information technologies, and DoD finds itself

following that lead.[3] DoD has become another consumer of information systems in a market driven by commercial imperatives rather than by the military's needs. This progress does not rest on congressional approval or disapproval of a defense budget, but rather on a strong commercial market. Thus, not only will information technologies continue to expand but they will be sold rapidly throughout the world and many state and non-state actors will choose to capitalize upon their potential as offensive weapons.[4]

Information technologies have done more than permanently alter conventional military forces - they have created a new dimension of conflict. General Fogleman and others have said that information dominance and winning information wars will be the prerequisite for victory in future conflicts.[5] Although Guilio Douhet made similar claims about airpower in the 1920s, his visionary projections of airpower failed to fully recognize the potential for countermeasures which would degrade airpower effectiveness. Whereas airpower did revolutionize warfare, it was not to the extent of Douhet's visions. The information revolution will most likely run a similar course.

The United States is at the very beginnings of a revolution in military affairs.[6] To understand this concept, it is important to distinguish between evolutionary and revolutionary change. In evolutionary change, progress is made by improving upon the last generation of military weapons, organizations, or tactics. It often takes the form of a seesaw battle between the development of new offensive capabilities followed quickly by the development of defensive countermeasures. First one is ascendant, then the other. Progress can be impressive but there still exists a continuity between the present and the past.[7]

Revolutionary change, on the other hand, results in is almost no continuity between the present and the past. What we are seeing is something entirely new. Revolutionary changes are

important because nations that recognize and exploit them usually defeat nations that do not.[8] Situations with the potential for revolutionary changes in warfare provide ambitious powers with an opportunity to become dominant or near dominant powers.[9] Both Germany and Japan were medium-sized powers as rated by gross national product, population, and other broad measures of national power at the commencement of World War II. However, Germany's development of blitzkrieg and Japan's dramatic reliance upon carrier airpower provided each with significant advantages during the war's opening years. Indeed, it was not until 1942 that the allies came to understand the significance of these two revolutionary developments in warfare and devised measures to counter them. The United States is once again faced with revolutionary change and, as it has in the past, such change could once again pose a threat to the nation.[10]

The concept of using information and information technology as a weapon is at the heart of the current revolution in military affairs. Until the United States understands this basic change in warfighting and devises appropriate countermeasures to defend itself, it will be vulnerable to actors who more quickly grasp the nature of this change and seek to exploit it. At present, the US defense establishment remains unchallenged in the four traditional dimensions of warfare. However, it likely will not be the primary defense mechanism in the fifth dimension, the information realm.

Information warfare as a new dimension of conflict provides unprecedented methods to directly impact a nation's will through information attacks that can circumvent many conventional military defenses. It will produce new forms of warfare quite different from the other four dimensions of conflict. The Air Force pamphlet, The Nation's Air Force Booklet, states, "Today, dominating the information spectrum has become as critical to conflict as occupying the land or

controlling the air has been in the past."[11] Superimposed across the traditional spectrum of warfare, information not only complements existing dimensions of warfare but itself creates a new dimension for exploitation. It represents yet another means of achieving political objectives.

Rapid Exploitation of Information Can Produce Advantages

> History does not teach that better technology necessarily leads to victory. Rather victory goes to the commander who uses technology better, or who can deny the enemy his technology.
>
> Office of the Chief of Naval Operations

Decision-making cycles tighten in the information age. Information delivers enormous power into the hands of any individual, anywhere on the globe, with the wits and interest to use it. Those who understand this new reality have the potential to get inside a competitor's decision making cycle and seize the initiative in combat or competition.

This has obvious benefits in warfare and commercial applications. These new technologies provide users with the potential to rapidly: 1) *Observe* with greater detail the reality of their environment; 2) *Orient* themselves with greater accuracy than someone with less information; 3) *Decide* with greater insights thereby greater accuracy; and 4) *Act* within a shorter timespan and with enhanced assertiveness.[12] This four-step paradigm entitled the OODA loop is one way of viewing decision cycles. Leaders (both civilian and military) who can effectively observe, orient, decide, and act faster than their opponent can seize the initiative in combat or competition and shape the battlefield by limiting and channeling an adversary's options. One writer called the US military's breathtaking speed in completing Desert Storm OODA loops "a sort of continuous temporal outflanking."[13]

This facet of OODA enhancement places greater pressures on senior leaders to respond

rapidly to changing conditions throughout the world. Shortened time lines for decision making are particularly significant in the arena of national security where today's decision makers, and those surrounding them, have a limited understanding of warfare or the capabilities of the military.[14] They also represent potential liabilities if the four-step OODA cycle is interrupted or a decision maker is forced to decide or act without adequate time to observe and orient. When British Prime Minister John Major was asked if leaders today are disadvantaged by the "CNN Syndrome" and if the demand for immediate response concerned him, he replied:

> It doesn't get on my nerves. It is a fact of life. I think it is bad for government. I think the idea that you automatically have to have a policy for everything before it happens and respond to things before you have had a chance to evaluate them properly isn't sensible.[15]

Presidential advisor George Stephanopoulis echoes Prime Minister Major's sentiments:

> In the White House...we have 24-hour news cycles...CNN assures that you are forced to react at any time, and that's going to happen throughout the time of the Clinton presidency.[16]

The national security advisor to former Vice President Dan Quayle was more specific:

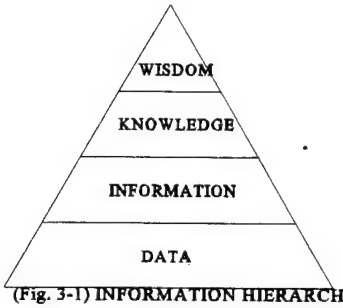
> There's really no time to digest this information so the reaction tends to be from the gut, just like the reaction of the man on the street. High level people are being forced essentially to act and to formulate responses or policy positions on the basis of information that is of very uncertain reliability.[17]

Using information techology to create advantages for decision makers by compressing the amount of time needed to gather data is an important advantage in warfare. Unless the data collected is free from contamination, however, it may also be a potential liability. Moreover, the same technology may be used to place an opponent at a disadvantage by forcing it to make rapid decisions based upon corrupted data. These concepts of speed and accuracy in decision making reveals the importance of protecting information.

Information Itself Must Be Protected

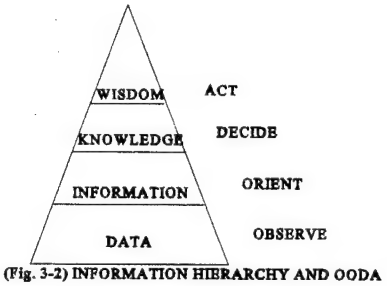
> Know the enemy and know yourself; in a hundred battles you will never be in peril.
>
> Sun Tzu

A generally accepted information hierarchy (figure 3-1) illustrates the importance of protecting information. At the bottom of this hierarchy is data that is defined as raw facts. It may include useful or irrelevant and redundant facts and must be processed to become meaningful. Information consists of the trends or patterns that emerge from quantities of processed data. The third layer is knowledge of the information provided, the circumstance of attempting to discern the truth through reasoning. Finally, there is wisdom, the epitome of the information hierarchy. Wisdom comes with gaining insight from knowledge.[18]



(Fig. 3-1) INFORMATION HIERARCHY.

These four levels of the information hierarchy relate to the OODA decision making cycle (figure 3-2). Data requires observation, then orientation to become information. Decision makers must then study the available information and apply reason to acquire knowledge. From such knowledge, hopefully wise decisions are made.[a 19]



(Fig. 3-2) INFORMATION HIERARCHY AND OODA

Corrupting either of the two bottom elements inevitably taints the elements above them and impacts the OODA decision making cycle. Therefore, protection of

---

[a] Col Boyd said that the most important part of the OODA loop is the orient phase. Orientation is the real starting point because it affects what we decide to observe and then what we decide to do based on what we observe.

data and information becomes critical to the integrity of knowledge and wisdom and to the accuracy and appropriateness of decision making.

History is replete with examples that demonstrate the damage done when the information used to make decisions is corrupted. For example, three days after D-Day in Normandy, Hitler was still holding German forces in the Pas de Calais area to repel the supposedly imminent landing of the Allied invasion force there. His decision was based upon inaccurate information that resulted from misleading data planted by the Allies.

Rapid decision making cycles and the vulnerability of data to corruption underscores the vulnerability of decision makers if either is manipulated by an opponent. As George Stein puts it:

> Information warfare is about the way humans think, and more importantly, the way humans make decisions. It is about influencing human beings and the decisions they make. Information warfare is real warfare, it is about using infor- mation to create such a mismatch between us and an opponent that, as Sun Tzu would argue, the opponents strategy would be defeated before his first forces can be deployed or his first shots fired. The target of information warfare, then, is the human mind, especially those minds that make the key decisions on if, when and how to employ assets and capabilities embedded in their strategic structures.[20]

The traditional method of guarding information is to limit physical access to it. The locked file cabinet and personal security clearances are products of current thinking about how to best limit the number of persons with the ability to peruse and use confidential or sensitive information. However, the information age is dramatically changing this equation and requires a change in our cultural thinking about security.

Modern information technology places a premium on electronic transmittal, processing and storage of information. America's wholehearted embrace of information technology has transferred huge quantities of private and sensitive information from the locked file cabinet onto

computer files accessible through information networks. The places where data and information reside (data bases, communications networks, logic programs) are alluring targets in a society heavily dependent upon them. In many significant, documented cases the desire to gain interconnectivity has not been balanced with an adequate concern for security, resulting in loss of confidentiality, integrity, or availability of the information (see appendix A for examples). The Director of the Defense Information Systems Agency observed that in protecting such information, "The most important way is making sure people use the right procedures and processes, and do not use shortcuts [in security]."[21] A Joint Security Commission report highlighted two areas for security emphasis: personnel security and security training.[22]

The conundrum national leaders must solve is to enhance security without limiting access. The answer requires at a minimum an assessment of relative information value and assignment of appropriate security measures to protect it. A simplified look at the issues involved in this relative ranking of value include: confidentiality - how critical is it that only authorized personnel view this information; integrity - how important is it that this information not be tampered with; and availability - how crucial is it that this information be available whenever it is needed. As Dr. James Hearn testified before the House Judiciary Committee, "We need to focus on the information to be protected, and its value, not on the mechanisms of protection."[23]

Further complicating the determination of appropriate security devices are issues of liability, public affairs, legality, personal rights for privacy or freedom of speech, and national security. Each of these frames of reference provide potentially different answers to the same set of questions. There must be a balance between the needs of the state and the rights of the individual, between the need to know and the need to maintain privacy.[24] Such an exercise

highlights the importance of a national security grand strategy built upon a consensus around these issues.

New Strategic Vulnerabilities Have Made Traditional Notions of US Physical Sanctuary Less Meaningful

> There is no geography or sanctuary in cyberspace.
> VADM Arthur Cebrowski, USN

The permeability of worldwide information systems reduces the relevance of the physical sanctuary that our nation has enjoyed for more than 200 years. Since its founding, the United States has rested safely behind the Atlantic and Pacific Oceans - its strategic centers of gravity safely protected by physical barriers. Since the end of World War II, standing conventional forces and a policy of deterrence have maintained this protective barrier even from the nuclear threat of the Cold War. Now, in this new dimension of warfare, physical sanctuary and reliance upon conventional military forces will not protect many US strategic centers of gravity from potential information attacks. As long as defensive countermeasures of information warfare lag behind innovative uses of the same technology, the US will have new strategic vulnerabilities.

For the time being, information technology holds the potential to become a great equalizer among nations. The efforts of vulnerable nations, a list the US tops, to create defensive countermeasures to information attacks will directly impact both the depth of such attacks as well as the number of potential information attackers. The window of vulnerability is only as big as those who are vulnerable allow it to be.

Actors Other Than Traditional Nation States Can Initiate Information Attacks

Who are those guys?
Butch Cassidy and the Sundance Kid, 1969

When considering the nature of the threat, Cold War mentality and measurement devices must be discarded. Information warfare can be executed with far less capital than needed for conventional conflicts. Large-scale conventional warfare requires taxing the resources of large populations to build the force structure; thus, only nation states have had the wherewithal to engage in it. Additionally, conventional warfare requires greater force structure and training expense than does the smaller elite cadre required of information warfare. Since the ante to enter information warfare is on a scale far below that for conventional warfare, potential attackers are not limited to traditional nation states.

One view is that anyone with an agenda, a modicum of training, and a small investment in equipment can launch an information attack.[25] Others disagree. However, although estimates needed to mount significantly disruptive attacks against information targets may vary, there is general consensus that the amount is well within the range of non-state actors, including groups and individuals.[26]

The emergence of these non-state actors represents perhaps the most significant threat to US national security interests in the foreseeable future. They could potentially launch an invisible electronic attack against the US without a shot being fired and without direct knowledge of who the adversary might be.[27]

New Strategic Measures of Effectiveness Are Needed to Prioritize Both Offensive and Defensive Efforts

Three elements determine the effectiveness of a national strategy. What is the strategic goal? How well is national power oriented to achieve the goal? What do the indicators show with respect to how well the nation is doing in achieving its goal? The answers to these questions, taken together, establish the planned measure of strategic effectiveness.[28] None exist for information age conflict strategies for either offensive or defensive information warfare.

It is important to differentiate between measures of effectiveness at the operational and strategic levels. The military may perform well at the operational level, but fail because those operations are not linked to a strategic goal. US military operations in Vietnam were an example of this disconnect. Talking to a senior North Vietnamese official after the war, a US Army officer observed that the United States military had never been defeated in combat. His North Vietnamese counterpart replied that while that was true, it was also irrelevant.[29] [30] The North Vietnamese officer was correct.[b]

Attrition is the strategic measure of effectiveness for traditional warfare. Presently, nations gauge progress toward achieving their war aims by measuring numbers of enemy killed, amounts of supplies destroyed, extent of the enemy infrastructure rendered unusable, transportation disrupted, and so forth. The ultimate goal of attrition warfare, is to destroy the

---

[b] In 1995, Christopher Jenner interviewed Gen. Nguyen Don Tu, an intelligence officer in the North Vietnamese Army who served as Gen. Dong's chief of staff during the 1968 TET campaign on Hue, and was also a member of the North's negotiation team at the Paris peace talks. Gen. Tu was author of a report, "How to Manipulate the U.S. Media." His knowledge of US political systems and civilian sensitivity was telling and he provided sound evidence of having put this to great effect in information warfare with the US in the Vietnam war. During an oral history conducted with MG Edward Lansdale in 1986, Mr. Jenner learned of Gen Tu and of his manipulation paper, that was subsequently distributed to a number of Communist countries, including Cuba. MG Landsdale held Gen Tu in high esteem as an adversary and considered him a brilliant information warfare exponent.

enemy's will to make war by destroying its physical warmaking capabilities. However, this measure of strategic effectiveness is inapplicable when the weapons used are not designed to bring about physical destruction. The effectiveness of information as a weapon cannot be measured readily by resorting to attrition methodologies. New measures of strategic effectiveness must be designed to assess both offensive and defensive information warfare.

Looking at the Vietnam War from North Vietnam's standpoint, one can argue that it is a good example of information warfare at the strategic level. It is logical to assume, particularly after the 1968 Tet Offensive, that North Vietnam could not hope to defeat the United States militarily on the battlefield. That did not mean, of course, as subsequent events proved, that North Vietnam was defeated; quite to the contrary. The effectiveness of the North's strategy was not measured in terms of attrition warfare but rather by the weakening of America's resolve to continue the struggle. They succeeded because they linked what national power they possessed to their strategic goal and focused all of their energies on attaining it.[c] But what indicators did they use to determine whether they were making progress? The number of anti-war newspaper articles? The size and fervor of American anti-war demonstrations? The speeches of anti-war politicians? Were these measures somehow formalized or simply a consensus of the gut feelings of North Vietnam's Politburo members?

Warfare in the information age requires new measures of strategic effectiveness that account for the impact of information technology on the enemy's leaders, government and population. The lack of these measures is a new reality that must be addressed by national

---

[c] Today, information technology would present the North Vitnamese with additional options to directly impact the weakening of US resolve.

security policymakers.

Synopsis of Information Age Realities

These six realities point to the fact that the grand strategy of national security built solely on conventional forces is out of date. The Department of Defense can not be the sole providers of national defense in the information age. ***Information technologies have created a fifth dimension of conflict***. Recognizing the uniqueness of this dimension highlights the limited relevance of the world's most powerful army, navy, and air force in defending strategic centers of strength from information attacks. The sum of their conventional forces is far more potent than any would challenge conventionally; but are an inadequate deterrent to deflect information weapons or protect information targets. In this new dimension, the ***rapid exploitation of information can produce significant advantages in warfare and in commercial competition.*** Leaders who exploit information technology may seize the initiative, get inside an opponent's decision making cycle, and thereby limit or channel the options available to the enemy. Moreover, in the information age interconnectivity and dispersed computing power have greatly expanded access and dependence upon information, making the places it resides (databases, communication networks, logic programs) more susceptible and attractive targets. Therefore, ***information itself must be protected.*** Information can be used as a weapon to corrupt or destroy or it can be the target of an attack. For as long as defensive countermeasures lag behind innovative use of offensive information weapons, the US will have ***new strategic vulnerabilities which make traditional notions of US physical sanctuary less meaningful***. Heavy US dependence upon information systems combined with today's worldwide interconnectivity of computer systems,

which have limited self-protection features, has created an avenue for attack of strategic assets. Financial institutions, public switch networks, power plants, and other strategic centers of strength could be at risk from information attacks and military conventional forces can do very little to protect them. Ample historical examples exist demonstrating the significant disruptions of information systems that can occur. Although many of these have been caused by computer logic errors, this does not preclude malevolent actors from intentionally seeking to cause such havoc to further a particular cause. Additionally, since the ante to enter information warfare is on a scale far below that for conventional warfare, ***potential attackers expand far beyond traditional nation states***. If the US is to effectively build and execute a new grand strategy for national security, efforts beyond the military must be employed and ***new strategic measures of effectiveness are needed to prioritize both these efforts in both the offensive and defensive categories.***

The following chapters build a proposal for a new strategic framework upon this foundation; an information age framework from which a new grand strategy for national security can be crafted.

1. SAIC, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, (Washington: SAIC, 1995) 2-19, 2-20, 4-1. The Computer Security Act of 1987 assigned responsibility for security standards and guidelines to the Department of Commerce, National Institute of Standards and Technology, National Security Agency, and General Services Administration. Executive Order 12356 established the Information Security Oversight Office, under the Office of Management and Budget, to oversee compliance with national security information guidance. Protection of civilian infrastructure by the Department of Defense is further complicated by the Posse Comitatus Act which limits the use of the military for enforcing the law of the land.

2. Kenneth C. Allard, "The Future of Command and Control: Toward a Paradigm of Information Warfare," Turning Point: The Gulf War and US Military Strategy," ed. L. Benjamin Ederington and Michael J. Mazaar, (Boulder: Westview Press, 1994) 161-192.

3. SAIC, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 4-1.

4. SAIC, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 4-2.

5. Lt Gen John S. Fairfield, "A Jointly Focused Vision," Armed Forces Journal, January (1996): 37; United States, Army, Concept for Information Operations, (Fort Monroe: TRADOC, Aug. 1995) 7; Gen. Ronald R. Fogleman, "Information Operations: The Fifth Dimension of Warfare," address, Armed Forces Communications-Electronics Association meeting, Washington, 25 Apr. 1995.

6. Marshall, memo, 1994.

7. Richard J. Dunn, III, From Gettysburg to the Gulf and Beyond: Coping with Revolutionary Technological Change in Land Warfare, (Washington: Institute for National Strategic Studies, McNair Paper 13, 1995) 3.

8. Dunn, 3; Jeff Barnett, "The Revolutions in Military Affairs," briefing slides (Washington: Office of Net Assessment, 1995).

9. Paul Wolfowitz quoted in Marshall, 3.

10. Dunn, 3.

11. United States, Air Force, The Nation's Air Force Booklet, (Washington: US Air Force, 1995) 11-12.

12. Col John R. Boyd, "A Discourse on Winning and Losing," briefing slides, (Maxwell Air Force Base, AL: Air University Library, 1987).

13. Oliver Morton, "The Information Advantage," The Economist, 10 Jun. 1995: 5.

14. James Adams, "The Role of the Media," lecture, Information Warfare Course, National Defense University, Washington, 17 Dec. 1995.

15. Thomas Plate and William Tuohy, "John Major; Even Under Fire, Britain's Prime Minister Holds His Own," Los Angeles Times, 20 Jun. 1993: M.3.

16. David S. Broder, "Looking Ahead in '92," Boston Globe 6 Apr. 1994: 15.

17. Carnes Lord, remarks recounted in Thomas J. McNulty, "Television's Impact on Executive Decisionmaking and Diplomacy," The Fletcher Forum of World Affairs, 17 (Winter 1993): 81-82.

18. John Arquilla and David Ronfeldt, "Information, Power, and Grand Strategy: In Athena's Camp," paper, Catigny Conference, Wheaton, IL, Jul. 1995, 6. The authors cite as the source of the diagram in Harlan Cleveland, The Knowledge Executive: Leadership in an Information Society, (New York: Dutton, 1985); Robert Lucky, Silicon Dreams: Information, Man and Machine, (New York: St Martin's Press, 1989). David Ronfeldt, Cyberocracy, Cyberspace and Cyberology: Political Effects of the Information Revolution, (Santa Monica: RAND, 1992) 4.

19. United States, Army, "Information Operations, FM 100-6," draft, (Fort Monroe, VA: TRADOC, Jan. 1996) 2-1, 2-2, 2-3, 4-1, 4-2, 4-3, 4-4; for same conclusion, see also Col Edward Mann, Thunder and Lightning--Desert Storm and the Airpower Debates, (Maxwell Air Force Base, AL: Air University Press, Apr. 1995) 152; Gen. Frederick M. Franks, address, Association of the United States Army Symposium, Orlando, FL, 8 Feb. 1994.

20. George Stein, "Information Warfare," Airpower Journal, (Spring 1995): 32.

21. Lt. Gen. Albert Edmonds, interview, Defense News, 16-22 Oct. 1995, 102.

22. Joint Security Commission, Redefining Security: a Report to Secretary of Defense and Director of Central Intelligence, (Washington: Joint Security Commission, Feb. 1994) vi.

23. United States Congress, House Judiciary Committee, "The Threat of Foreign Economic Espionage to US Corporations," Testimony by Dr. Hearn, 29 Apr.-7 May 1992, Washington: GPO, 1992, 87.

24. SAIC, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 4-1.

25. Ronald Grove, "The Information Warfare Challenges of a National Infrastructure," paper, InfoCon symposium, Washington, Sep. 95, 9.

26. Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War," draft, (Santa Monica: RAND, 1995) xvi; United States, Dept. of Defense, Defense Science Board, 52.

27. SAIC, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2-66.

28. Stephen P. Rosen, Winning the Next War, (Ithaca: Cornell University Press, 1994) 35.

29. Harry G. Summers, On Strategy: A Critical Analysis of the Vietnam War, (Novato, CA: Presidio Press, 1982) 1.

30. Christopher Jenner, memorandum to authors, March 1996. Notes from Christopher Jenner regarding personal interview with General Nguyen Don Tu, 1995; and personal interview for an oral history conducted with MG Edward Lansdale, 1986.

Chapter 4: A Strategic Framework

Centers of Gravity: Nation States Viewed as Systems

Col. John A. Warden III, USAF (retired), a modern strategic thinker, asserts that today's industrial nations must be viewed as systems that derive their national power from five centers of gravity each of which is critical to the state's existence.[1] Combined they produce a synergy from which national power emerges. According to Warden, modern strategic warfare must focus on this system as a whole with the purpose of forcing changes in one or more of its centers of gravity. Such changes, he contends, will produce disruptions in the nation as a system and lead to changes in its policies or to its physical inability to continue resistance.[2] Like Clausewitz, Warden believes the purpose of war is to compel the enemy's submission.

Warden's centers of gravity, also depicted in figure 4-1, consist of the following:

- A nation's **leaders,** civilian or military, who have the authority to commit their country to war, prolong its resistance or lead it to peace.
- **System essentials** are the resources or facilities without which a nation cannot maintain itself. They are not necessarily defense related or contained within the boundaries of a nation. In many cases they may be the most critical nodes within these resources or facilities.[a]
- The **infrastructure** consists of a nation's system for moving goods and services. Roads, bridges, airports, rail lines, and ports all fall within this category. This also contains portions of a nation's industry that are not considered system essentials.
- A nation's **population.** A nation's citizens, whether within or outside of the nation's borders.[b]

---

[a] Warden places telecommunications in the leadership ring. We have elected to place it in the system essentials category.

[b] As Clausewitz, Sun Tzu, Churchill and Ho Chi Minh knew, "In war there are two factors, human beings and weapons. Ultimately though, the human beings are the deciding factors." Gen Vo Nguyen Giap. This lesson has been

- The **defense mechanism** consists of military forces. The nation's defense systems protect the nation from external and internal threats. They also shield other centers of gravity from attack and threaten the centers of gravity of competitor states. They include law enforcement and intelligence agencies.

Leadership	System Essentials	Infrastructure	Population	Defense Mechanism
Government: National Leadership (NCA, Congress, Cabinet)	Critical nodes of: telecom systems, power and petroleum distribution systems, financial system, trade	transportation systems, R&D facilities, key production, media, retail, health, education, entertainment	Citizens	Military forces, Law enforcement agencies, intel activities

(Fig. 4-1) The nation as a system, depicting a nation's five strategic centers of gravity as a matrix.

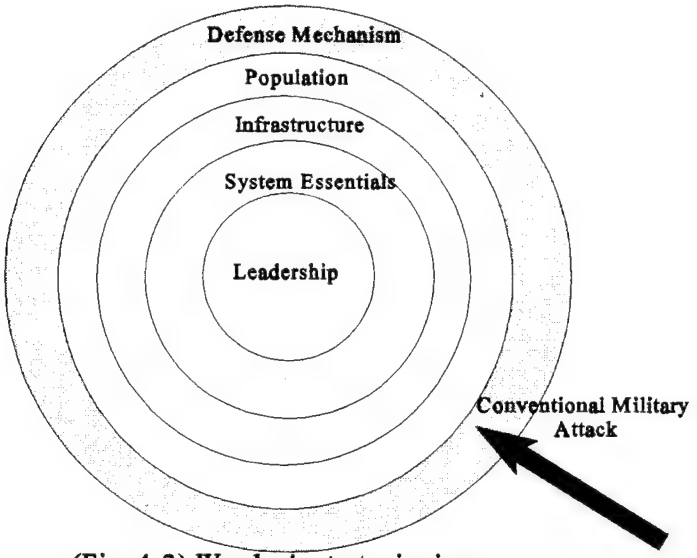
The Relative Importance of Strategic Centers of Gravity

Depicting a nation's centers of gravity as five concentric circles, or strategic rings, illustrates their relative importance (figure 4-2). At the center of this model is the nation's leadership. It occupies the most protected position because it alone can make the decisions that lead a country into or away from war. Surrounding it, in descending order of importance, are system essentials, the infrastructure, and the population. The outermost strategic ring, the defense mechanism, is the most resistant to attack and acts as an outer shell. Its function is to guard and protect the other strategic rings from external attack or degradation and to promote the nation's policies by threatening the strategic rings of competitor nations.[3] The outermost, or military ring, is the most important center of gravity in conventional warfare because it protects the other more vulnerable centers. Once the military ring is penetrated, a nation's inner core becomes exposed and its leaders face a Hobson's choice of either submission or annihilation. Accordingly, for

---

learned by US opponents in Somalia, Bosnia, Libya, Iran and Iraq.

disciples of Clausewitz, the objective of violence is to disarm an enemy's military forces.



(Fig. 4-2) Warden's strategic rings.

The Fifth Dimension Presents Both Opportunities and Vulnerabilities

Permeability and access characterize the fifth dimension and present strategic planners with new opportunities, new vulnerabilities and new grand strategy options. Comprehending what is new requires an understanding of what has changed. In the past, nation states conducted military operations in four dimensions (land, sea, air, and space) to reach the enemy's internal strategic rings (Figure 4-2). Evolving weapons technology has provided a limited ability to leapfrog an enemy's protective outer shell on occasion and directly attack its more critical centers of gravity.[c] In response, nations have constructed more physical barriers in the skies and in space

---

[c] During the Gulf War, Iraq was able to attack the fifth US strategic ring, its fighting mechanism, the only ring to which it could obtain access. Examples of Iraqi information attacks using perception management techniques include Saddam Hussein's use of a 7 year old boy during a human shield propaganda demonstration, the display of civilian casualties and the destroyed "Baby milk factory" on CNN.

The UK sustained attacks to all rings during the bombing and missile attacks in WWII. Germany damaged Britain's leadership, system essentials and infrastructure while targeting its fourth strategic ring, the population.

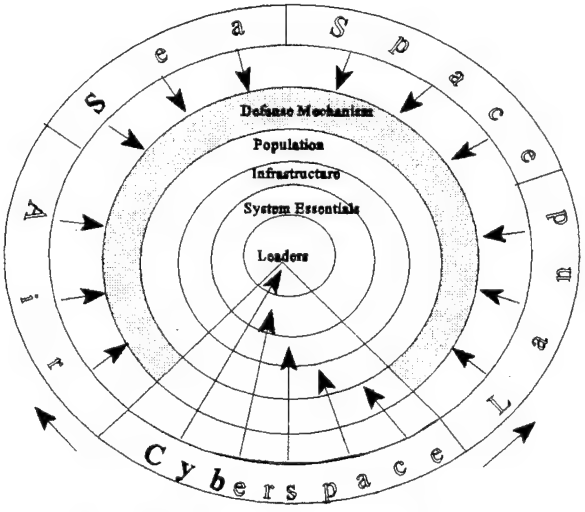
in the form of air and missile defenses. These provide a reasonable measure of protection against traditional attacks. In most instances, these defenses along with constraints in time, space or resources prevent a nation from effectively attacking more than one or two of an enemy's strategic rings.[4]

Time, space and resources are also constraints in a military campaign (a series of related military operations aimed at accomplishing a strategic or operational objective within a given time and space[5]). Amassing the amount of conventional hardware and delivery systems necessary to launch simultaneous attacks against all five strategic rings is difficult, if not prohibitive. A result is that nations fighting in the four existing dimensions of warfare husband their warfighting assets, assess enemy vulnerabilities, and carefully prioritize targets for attack. This prioritization makes the outermost strategic ring, the fighting mechanism, paramount as a target, because as long as it remains a viable fighting force that can protect the state's more vital centers of gravity, the nation cannot be subdued.

The permeability of traditional defense mechanisms to information attack with the consequent increase in access to enemy strategic centers of gravity has significant ramifications for planners of grand strategy. Physical defeat of an enemy's military forces may no longer be necessary to gain direct access to its more vulnerable inner strategic rings. Simultaneous attacks against multiple centers of gravity become possible because the weaponry (information) and the delivery means (networked computers) are relatively cheap and plentiful. Moreover, while traditional modern weapons remain capable of destroying computer systems that serve as offensive information weapons, the sheer number of potential weapon systems involved may make it difficult to eliminate or substantially degrade an opponent's arsenal. Finally, defensive grand

strategists must take note that nation states other than those possessing conventional military power and non-state actors may have the potential to attack vital centers of gravity.

Figure 4-3 suggests the permeability of the information realm and the increased access it provides to a nation's inner strategic rings. The depiction is not to suggest access will be unopposed or the existence of a strategic model that is indefensible. On the contrary, as previously noted, the capability of an opponent to successfully penetrate to strategic centers of gravity with information weapons will depend upon the vigilance and defenses of the targeted nation. The development of effective countermeasures is likely to be the product of first recognizing the threat and then developing appropriate defenses. The danger to the United States centers of gravity lies in the period before such countermeasures are in place.



(Fig. 4-3) The fifth dimension of warfare.

Weapons for Attacking the Intangible

Information weapons attack targets in three ways: physical destruction, alteration of the target's internal operating logic and manipulation of the target to produce behavioral changes.

For ease of reference, these three categories are called destruction, corruption and perception management.[6]

Physical Destruction Remains a Means of Attack

Attacks using conventional weapons systems remain important strategically because they target physical assets of the enemy's strategic centers of gravity. In the information realm, they destroy the electronic components of information systems, i.e., switches, trunk wires, major databases and other key physical information nodes.[7]

Weapons Category	Weapons Function	Weapons Type
Destruction	Physical destruction of targets	Conventional weapons

(Fig. 4-4) **Physical destruction** attacks the electronic components of a nation's information systems.

Though iron bombs themselves are not normally perceived as information weapons, it is important to remember that it is their effects upon the target which concern us, not their technical capabilities. If successful, iron bombs against an information node deny the enemy use of the information it processes. Hence, "(B)ombing a telephone switching facility is information warfare. So is destroying the switching facility's software."[8]

Targeting information functions for physical destruction is likely to produce new attack strategies aimed at dismantling systems that are heavily dependent upon electronic information systems to function, i.e., electricity, water, natural gas, transportation and broadcasting systems. War planners have the option of not having to target an entire system but rather targeting only those critical pieces that process the information controlling it.

Corruption: A New Method of Targeting Information and Information Based Systems

Corruption weapons operate by controlling or disabling the internal operating logic of the targeted networks and systems.[9]

Weapons Category	Weapons Function	Weapons Type
Corruption	Disruption of internal operating logic	Viruses of all types, HERF guns, EMPT bombs, filters, and agents

(Fig.4-5) **Corruption** alters the internal operating logic of the targeted networks and systems.

Viruses, chipping,[d] sniffers,[e] HERF guns,[f] EMPT bombs,[g] their numerous variants and mutations all fall within this category. These weapons are important because they control an enemy's information systems by controlling their internal operating logic. Such control means control of an enemy's decision making process and of his awareness and understanding of his environment.[10] Physical destruction of these systems, with the concomitant need to reconstruct them at war's end, is no longer required. Given the devastating power of modern weapons systems, defeat of an enemy without inflicting massive collateral damage, that inhibits the enemy

---

[d] The modification, alteration, design, or use of integrated circuits for purposes other than those originally intended by the designers. A chip that is meant to fail, or to act differently than it is supposed to. Schwartau, 164.

[e] Software programs designed to analyze a communications network. They diagnose problems and assist network administrators in fixing them. In some cases, the software is written so that network administrators are unaware someone else is snooping through their networks collecting information, such as passwords, tapping databases, and listening in on telecommunications transmissions. Sniffers may be written to ferret out information which will permit the user to surreptitiously enter and/or manipulate the system later on. Schwartau, 116.

[f] A high energy radio frequency (HERF) gun is a radio transmitter like device that shoots a high powered radio signal at an electronic target sufficient to disable it at least temporarily. HERF guns work by overloading the target's internal electronic circuits. Schwartau, 178-179.

[g] A non-nuclear, electromagnetic warhead that produces powerful, electromagnetic radiation. The resulting electric and magnetic fields overload and destroy electrical and electronic systems within the range of the weapon. The signals are sufficiently strong to disable any computer in their path permanently as well as destroy any floppy diskettes, hard disks, tapes and backup tapes nearby. Schwartau, 180-181.

population's ability to sustain itself, is much preferred to the costs of rebuilding a country following its destruction from traditional attacks.

Perception Management: Improved Means of Targeting a Population

Perception management seeks to effect what an opponent's targeted information systems portray as reality.[11] In some respects, it is analogous to the effects produced by psychological or deception operations. However, the access which modern information technology provides to enemy centers of gravity has made it much more.

Weapons Category	Weapons Function	Weapons Type
Perception Management	Behavior	Spamming, spoofing, misinformation, discourse, slogans, arguments, information overload

(Fig. 4-6) **Perception management** affects what an opponent's targeted information systems portray as reality.

Perception management can be clandestine or open, manipulative or straight-forward. It can occur over an extended period of time or during an instant, perhaps at the critical moment during a crises. It can be broad based or targeted with the precision of a rifle shot. It presents both great opportunities and great vulnerabilities. Selective spamming,[h] spoofing[i] and misinformation are examples of perception management operations seeking to portray information as other than what it actually is.[12] The objective is usually short term and likely to be a specific decision or decision maker.

Slogans, promulgating specific arguments, injecting favorable points of view into public

---

[h] Using technology to "take over" a broadcast and replace the images shown with one's own program.

[i] Electronically altering images or words to convey a meaning other than intended by the subject being filmed or photographed.

discourse, and media manipulation (the "CNN factor"[13]) are open forms of perception management the effects of which are likely to be longer lasting. Precipitous swings in public sentiment, produced by the emotional closeness of watching dramatic events, are increasingly driving the national agenda as political leaders shift from one crises or controversy to the next.[j] Accelerated decision making cycles increase the chances of serious mistakes as people struggle to deal with increasingly complex matters during shorter time frames.

The importance of perception management is growing. Information technology is changing the world from one in which information control was relatively easy to one in which it is now virtually impossible. This change has had corrosive effects upon hierarchial institutions and governments which have relied, in whole or in part, upon control of information to maintain their status in the existing order.[13] Communism collapsed, in part, because the information revolution forced its governments to face a choice between openness and the possibility of their own demise or perpetual economic impoverishment and increasing civil upheaval.[k 14]

Centers of Gravity and Weapons Categories Form a Basic Framework

A nation's five strategic centers of gravity (figure 4-1) and the classification of weapon systems by function (figures 4-4, 4-5 and 4-6) provide the basic data needed to begin building a

---

[j] America has recently experienced the "CNN factor," increasing the public's emotional participation by showing dramatic events for spectators direct viewing. The result can be a loss of viewer objectivity.

[k] The Soviet experience suggests totalitarian governments cannot embrace information technology and maintain a closed society. Thus information technology represents a threat to both open and closed societies for different reasons. The more open a society, the more information technology will be used and dependence upon it will grow. The higher the dependence the greater the vulnerability to information attacks. The more totalitarian the society the more information technology must be resisted. As information technology is embraced, maintaining internal control of information becomes more difficult and the society grows more vulnerable to democracy.

strategic framework. Juxtaposing these two data sets produces a matrix from which the nature and scope the battlefield begins to emerge (figure 4-7).

	Leaders Government	**System Essentials** Critical nodes of: Energy distribution, telecom systems finance	**Infrastructure** Transportation, key production	**Population** Citizens	**Defense Mechanism** Military forces, LEAs
Destruction Physical destruction	Conventional weapons.				
Corruption Internal operating logic	Viruses of all types, HERF guns, EMPT bombs, filters, agents.				
Perception Management Behavior	Spamming, spoofing, misinformation, discourse, arguments, slogans, information overload.				

(Fig. 4-7) A basic information age strategic framework.

The Framework Shows the Existence of New Strategic Options in the Information Age

The extension of warfare to the information dimension and the permeability of that dimension presents strategic planners with options not presently available. Information technology now provides additional methodologies to isolate enemy decision makers from their own forces and populations by corrupting or denying use of their command, control and communications systems. Manipulation of popular perceptions also offers the opportunity to force enemy leadership into situations where it must divert from a confrontational course of action or face significant opposition or severe civil unrest within its own borders.

Comparing the relationships between national centers of gravity and weapons classes also helps the strategist visualize the total battlefield and to weigh available options between the use of

conventional versus information weapons. For example, some weapons are likely to be more effective than others against particular enemy centers of gravity. How much more effective, of course, depends upon the capabilities of the particular weapons systems at any given time relative to the alternatives.

Ignoring a Target is Also an Option

Not attacking a specific center of gravity or a "subsystem" within it is also a possibility which the strategic planner should not ignore. Indeed the addition of information technologies to warfare has simultaneously increased our understanding of an enemy's critical systems and at the same time provided more weapons with which to strike them. These capabilities enhance effectiveness by enabling war planners to attack critical enemy targets while allowing less critical others to be ignored. Thus "ignore" should be added to any matrix attempting to depict a relationship between weapons and targets.

Using the Basic Framework to Create Target Options

The basic strategic framework is adaptable and enables the strategic planner to quickly visualize options for implementing grand strategy. To illustrate, let us modify our strategic framework slightly to create a target matrix. Such a matrix, initially at least, would probably look something like figure 4-8. The significance of using the strategic framework in this manner is that it assists the strategist in crafting appropriate responses to different situations.

Take an enemy population as an example of how the target matrix might be used. In any conflict an enemy population is a difficult target to attack with traditional weapons. There are

simply too many targets and a population, particularly in an authoritarian state, is likely to suffer grievously without effect on the country's decision makers.[15] There is the additional argument that massive strikes against a civilian population may actually stiffen its will to resist the enemy. These considerations and the theories of air proponent Giulio Douhet aside, moral objections by the American people would likely preclude the United States from launching massive conventional attacks against a foreign population.

	Leaders Government	**System Essentials** Critical nodes of: Energy distribution, telecom systems, finance	**Infrastructure** Transportation, key production	**Population** Citizens	**Defense Mechanism** Military forces, LEAs
Destruction Physical Destruction	X	X	X		X
Corruption Internal Operating Logic	X	X	X	X	X
Perception Management Behavior	X			X	X
Ignore	X	X	X	X	X

(Fig.4-8) Comparing the relationships between national centers of gravity and weapons categories helps visualize the battlefield and weigh available options between the use of conventional or information weapons.

However, while physical destruction of an enemy population is an unlikely option, the framework suggests alternative methods for breaking its morale. Information weapons capable of corrupting or denying the use of information systems that drive the machines providing essential services to the enemy population, such as electrical, fuel or food distribution systems, public transportation or private financial transactions may provide an option for the strategic planner. Such weapons, by causing severe disruption to the target population, may well generate sufficient

internal pressures to force changes in an enemy's policy or leadership. In addition, efforts to manage the target population's perception of what is happening and why may be an effective or complementary strategy option.

Using the Framework to Create a Weapons Effects Matrix

Modifying the strategic framework with weapons effects produces an effects matrix as shown in figure 4-9.

	Leaders Government	**System Essentials** Critical nodes of: Energy distribution, telecom systems, finance	**Infrastructure** Transportation, key production	**Population** Citizens	**Defense Mechanism** Military forces, LEAs
Destruction Physical Destruction	-Elimination or isolation of leadership -Slows decision making	-Denial of service -Ripple effects -Isolates	-Creation of bottlenecks -Inhibits concentration of forces -Isolates	-Demoralize -Loss of will to fight -Stiffens resistance	-Disarms -Uncovers other centers of gravity
Corruption Internal Operating Logic	-Produces unwise decisions -Loss of popular confidence -Isolation -Misperception of events	-Interruption/ denial of service -Loss of confidence	-Creates bottle-necks -Inhibits concentration of forces -Isolation	-Creates confusion -Loss of security -Diverts energy -Promotes anxiety	-Produces unwise decisions -Isolation of leaders -Misperception of events -Failure of weapons
Perception Management Behavior	-Produces favorable decisions			-Produces pressures/ demands on leaders -Creates divisions -Manipulate passions	-Misperception of events -Produces unwise decisions -Creates divisions
Ignore	-Deemphasize damage	-Hide extent of damage	-Minor or inconsequential damage	-Control panic - Perception management	-Protect intel sources

(Fig. 4-9) A weapons effects matrix for the strategic battlefield.

The purpose of this exercise is not to suggest the effects noted in the matrix will always occur, but to show the framework as a tool with which strategists can begin to think about the use of weapon systems and their strategic implications ***and how these same concepts can be used against the United States, in the commercial, government and military sectors of the strategic centers of gravity***.

1. John A. Warden III, "The Enemy as a System," Airpower Journal (Spring, 1995): 47.

2. Warden, 43.

3. Warden, 46.

4. Warden, 51.

5. United States, Department of Defense, Joint Publication 3-0, Doctrine for Joint Operations (Washington: The Joint Staff, 1 Feb. 1995), GL-3.

6. Martin C. Libicki, The Mesh and the Net, (Washington: Institute for National Strategic Studies, National Defense University, McNair Paper 29, Mar. 1994), 56-57.

7. R. Garigue, "Information Warfare: Developing a Conceptual Framework," draft discussion paper, version 2.0, (Ottawa: Office of the Assistant Deputy Minister, Defense Information Services, 23 Aug. 1995) 32.

8. Ronald R. Fogleman and Sheila E. Widnall, Cornerstones of Information Warfare, (Washington: HQ USAF, 1995) 4.

9. Libicki, 57; Garigue, 33.

10. Garigue, 34.

11. Libicki, 58; Garigue, 34.

12. Garigue, 35.

13. Garigue, 35.

13. Carl H. Builder, "Rethinking National Security and the Role of the Military," unpublished article, (Santa Monica: RAND, 6 Sep. 1995) 14.

14. Builder, 10.

15. Warden, 50.

CHAPTER 5: Using the Framework to Analyze Information Conflicts

Primary Target in Clausewitzian Grand Strategy Changes From the Military to the People

The most effective grand strategy for offensive campaigns against an information age society is one that focuses on destabilizing the Clausewitzian trinity by attacking the "people" rather than the "military." Information age governments are especially susceptible not only to perception management weapons; but also to public pressure generated by corruption and destruction weapons.

As previously noted, examples of information system failures caused by malevolent actors are continuing to mount. If such disruptions are occurring, it is both reasonable and prudent to assume that malevolent actors will eventually attempt to exploit vulnerabilities in unprotected information systems to achieve political objectives through a structured information attack. This is the assumption underlying the RAND wargame. It is supported by the findings of a Defense Science Board report that describes the kind of threat the US is likely to face in future conflicts.[1]

System Essentials category targets like electrical power and telecommunication public switch networks have been repeatedly highlighted as susceptible to attack. The Congressional Office of Technology Assessment wrote that US electrical systems are "vulnerable to terrorist attacks." Although no attacks have ever caused widespread blackouts, the OTA concluded "there are reasons for concern that the situation may worsen."[2] Its report cites examples of significant hostile power system disruptions in Latin America, Africa, and Europe. Likewise, a National Communications System report, issued in January 1996, voiced even more concern about the vulnerability of US public switch networks.

> The last NSIE [National Security Intelligence Estimate] risk assessment in 1993 concluded that the risk to the Public Switch Network (PSN) from electronic intrusions was a serious concern. The NSIE representatives believe that in 1995 the overall risk to the PN [sic] from electronic intrusions is greater than that reported in the 1993 risk assessment, on the basis that threats are outpacing our deterrents while vulnerabilities are outpacing the implementation of protection measures.[3]

Energy provided through natural gas pipeline has also become telecommunications dependant. Federal regulations have dictated a national standard to maintain the crucial linepack[a] pressure balance throughout the nation's pipelines. Federally designed "electronic bulletin boards" manage a daily balance between what local delivery companies take out of the pipelines and what suppliers put into the lines. The Federal Energy Regulatory Commission Chair, Elizabeth Moler, has said the electronic bulletin boards are key in providing "both an early alert to changing conditions and a channel for instantaneous communication throughout an emergency."[4] This coordination capability, used in both daily operations and emergencies, would be lost without telecommunications system support.

The technical capabilities required to produce the incidents used in the RAND "Day After" exercise already exist. Figure 5-1 provides examples of similar real world events for each wargame incident. The actual incidents listed below demonstrate the credibility of the RAND assumption. Each incident is more fully described in appendix B.

---

[a]Linepack is the amount of gas maintained in the pipeline system. Lower tolerances are established to ensure delivery capacity, higher tolerances are set to prevent safety compromises.

Incident Number	Type of Attack	Similar World Event
3. Cairo Power Outage	Logic Bomb	Computer Espionage
4. CA and OR PSN Shutdown	Trap Door	LOD Time Bomb
5. Ft Lewis mass dialing attack	Info Overload	Noted Intruder Skills
6. ARAMCO Explosion	Logic Bomb	Kevin Poulsen Pleas Guilty
8. Metroliner Crash	Logic Bomb	1995 Arizona Railway Incident
10. Bank of England	Sniffers	Citibank $10 million Fraud Case
14. TPFDL Pollution	Virus	Paid Informants
15. Bank ATMs malfunction	Logic Bomb	$70 Million Software Glitch
19. Airplane Crash	Logic Bomb	Disgruntled Def. Contractor Emp.
20. Saudi News Takeover	Spamming	Demonstrated Technology
21. Saudi PSN Shutdown	Logic Bomb	Kevin Poulsen Pleas Guilty
23. IW Attacks Against US Bases	Multiple Efforts	DISA Red Team Results
25. JSTARS Malfunction	Worm	Electronic Intruders
26. D.C./Balt Phone Shutdown	Logic Bomb	Other Phone System Failures
27. Chicago Exchange Fluctuations	Logic Bomb	Shutdown Options
28. CBS News Takeover	Spoofing	Demonstrated Technology

(Fig. 5-1) RAND Wargame Incident Comparison

Applying the framework built in chapter 4 to the RAND game shows that the enemy made a concerted effort to attack the information systems that control the US system essentials. These are services, telecommunications and banking, vital to the nation's survival and upon which millions of Americans depend. The purpose of these attacks was to produce secondary impacts upon the US population, grossly disproportionate to the actual physical damage inflicted, and thereby create pressures on US leaders to alter their chosen course.

Three Step Framework Methodology

A methodology for applying the framework consists of three steps:

- Identify information attacks by weapons category
- Portray those attacks against the nation's strategic centers of gravity.
- Develop a weapons effects matrix.

Application of the framework to the RAND wargame, "The Day After...in Cyberspace," provides a good example of how the framework may be used.

Identifying Weapons Categories and Strategic Centers of Gravity in the RAND Wargame

Figure 5-2 lists 23 separate information conflict incidents that occurred during the "crisis" phase of the RAND wargame.[b] They illustrate the types of information attacks predicted by the Defense Science Board and are useful in demonstrating how to use the framework. For each example, the weapons category and target center of gravity has been identified. Examples of destructive attacks using conventional weapons have been deliberately omitted.

Decision makers must use personal judgment when determining appropriate centers of gravity classification for particular targets; this is especially true in the case of system essentials. Some systems, for example telecommunications, might be part of the system essentials for more developed countries such as the United States, while for others they might not.

---

[b] See appendix B for description of the 28 incidents occurring during the "crisis" period of the RAND exercise.

Incident Number	Type of Attack	Wpns Cat	Tgt Ctr of Gravity
3. Cairo Power Outage	Logic Bomb	Corruption	System Essential
4. CA and OR PSN Shutdown	Trap Door	Corruption	System Essential
5. Ft Lewis mass dialing attack	Info Overload	Corruption	Defense Mechanism
6. ARAMCO Explosion	Logic Bomb	Corruption	System Essentials
8. Metroliner Crash	Logic Bomb	Corruption	Infrastructure
9. Iranian Ambassador Statement	Discourse	Perc Mgmt	Leaders
10. Bank of England	Sniffers	Corruption	System Essentials
11. CNN "Financial Targets" Report	Persuasion	Perc Mgmt	Population
12. CPP Press Release	Slogans	Perc Mgmt	Population
14. TPFDL Pollution	Virus	Corruption	Defense Mechanism
15. Bank ATMs malfunction	Logic Bomb	Corruption	System Essentials
16. CNN Govt Coverup Report	Persuasion	Perc Mgmt	Population
18. CPP Demonstration	Slogans	Perc Mgmt	Leaders
19. Airplane Crash	Logic Bomb	Corruption	Infrastructure
20. Saudi News Takeover	Spamming	Perc Mgmt	Population
21. Saudi PSN Shutdown	Logic Bomb	Corruption	System Essentials
22. Saudi TV Announces Coup	Misinformation	Perc Mgmt	Population
23. IW Attacks Against US Bases	Multiple Efforts	Corruption	Defense Mechanism
24. CPP News Conference	Argument	Perc Mgmt	Population
25. JSTARS Malfunction	Worm	Corruption	Defense Mechanism
26. D.C./Balt Phone Shutdown	Logic Bomb	Corruption	System Essentials
27. Chicago Exchange Fluctuations	Logic Bomb	Corruption	System Essentials
28. CBS News Takeover	Spoofing	Perc Mgmt	Population

(Fig.5-2) Illustrative incidents from RAND wargame "The Day After...in Cyberspace."

Using the Framework to Analyze The Enemy's Information Targets

Having identified categories of weapons and centers of gravity, placing them within the context of the basic framework enables one to begin an analysis of the attacks. Patterns begin to appear from which the outlines of the conflict begin to emerge (figure 5-3).

	Leaders	System Ess	Infrastructure	Population	Def Mech
Destruction Physical Destruction					
Corruption Internal Operating Logic		3 Cairo Pwr 4 CA/OR PSNs 6 ARAMCO 10 Bank of Eng 15 ATMs 21 Saudi PSNs 26 DC/Bal PSN 27 Chicago Trd	8 Metroliner 19 Airplane		5 Ft Lewis 14 TPFDL 23 IW Attks 25 JSTARS
Perception Management Behavior	9 Iran Ambass 18 CPP Demo			11 CNN Rpt 12 CPP Pr Rel 16 CNN Rpt 20 Saudi News 22 Saudi Coup 24 CPP News 28 CBS News	
Ignore					

(Fig. 5-3) Illustrative information incidents placed in framework.

From the representative attacks which appear in the framework, it appears the enemy in the RAND scenario, has targeted the majority of its corruption weapons at the information systems controlling system essentials.[c] These are most likely civilian-owned and controlled systems and hence may not have the greater measure of protection likely to exist within the

[c] This initial impression taken from representative samples of the information incidents, such as one might expect during the initial stages of a conflict, is confirmed by a post conflict analysis of all information incidents in the context of the framework. See appendix B.

defense establishment. Added to this vulnerability is the fact that these systems, by definition, control essential services upon which untold numbers of the population depend. The effects of successful attacks upon them reverberate far beyond the mere shutdown of the individual systems.

Using the Framework to Analyze Weapons Effects

The next step in applying the framework is to develop a weapons effects matrix that is helpful in developing grand strategy in the information age. Using the framework to identify target centers of gravity moves the analysis into the sphere of grand strategy. Since the object of warfare is to compel human beings to submit to the will of other human beings, identifying the people most likely to be affected by these weapons provides an important indicator of how an enemy might pursue its grand strategy.

At the strategic level, the employment of all weapons of war have purposes beyond the immediate impact of the weapon itself. For example, bombs dropped to destroy a bridge not only have the purpose of destroying the bridge but also of disrupting the transportation stream which uses the bridge. The same is true of information weapons. Hence, at the strategic level information weapons, like conventional ones, are likely to produce effects on more than one center of gravity.

	Leaders	System Ess	Infrastructure	Population	Def Mech
Destruction Physical Destruction		6 ARAMCO	8 Metroliner 19 Airplane	8 Metroliner 19 Airplane	
Corruption Internal Operating Logic		3 Cairo Pwr 4 CA/OR PSNs 5 Ft Lewis 6 ARAMCO 10 Bank of Eng 15 ATMs 21 Saudi PSNs 23 IW Attks 26 DC/Bal PSN 27 Chicago Trd	8 Metroliner 19 Airplane	3 Cairo Pwr 4 CA/OR PSNs 15 ATMs 21 Saudi PSNs 26 DC/Bal PSN 27 Chicago Trd	5 Ft Lewis 14 TPFDL 23 IW Attks 25 JSTARS
Perception Management Behavior	3 Cairo Pwr 4 CA/OR PSNs 5 Ft Lewis 6 ARAMCO 8 Metroliner 9 Iran Ambass 10 Bank of Eng 11 CNN Rpt 12 CPP Pr Rel 14 TPFDL 15 ATMs 16 CNN Rpt 18 CPP Demo 19 Airplane 20 Saudi News 21 Saudi PSNs 22 Saudi Coup 23 IW Attks 24 CPP News 26 DC/Bal PSN 27 Chicago Trd 28 CBS News			8 Metroliner 10 Bank of Eng 11 CNN Rpt 12 CPP Pr Rel 15 ATMs 16 CNN Rpt 19 Airplane 20 Saudi News 21 Saudi PSNs 22 Saudi Coup 24 CPP News 26 DC/Bal PSN 27 Chicago Trd 28 CBS News	5 Ft Lewis 14 TPFDL 23 IW Attks 25 JSTARS
Ignore					

(Fig. 5-4) Using the framework to identify where the effects of information weapons fall.

Figure 5-4 shows the centers of gravity upon which the effects of our illustrative examples will land. Using the framework to identify weapons effects immediately underscores the ramifications of information conflict for the nation's leaders.

Secondary Impact of Information Attacks On Population Produces Pressure on Leaders

Attacks upon information systems which successfully disrupt services to the population

produce public pressures upon political leaders to act. Perception management and corruption weapons can combine to cause significant disruptions of normal daily activities which, in turn, generates:

- public anger over the government's inability to provide protection against such weapons;
- public anxiety about the potential consequences of demonstrated vulnerabilities;
- international questioning of US credibility.

This discontent can become a driving force to change national policies.

The fate of the American hostages in Iran is an example of how US public opinion can force decisions at the national level. As the weeks dragged by with no resolution of the Americans being held at the US Embassy in Tehran, public pressure within the United States began to mount for President Carter's Administration to take some action. One result of this pressure was the decision to launch the hostage rescue attempt that ended in disaster and the loss of American life at Desert One.[5]

A hypothetical incident in the RAND wargame illustrates the point. As an ally of the United States, Great Britain is also the subject of information attacks. The Bank of England discovers the presence of "sniffers" in its electronic funds transfer system. Immediate ramifications are that Britain suspects it is under attack because of its alliance with the US. CNN broadcasts a report of the attack (incident 11) which produces an immediate 10% drop in the stock market because institutional investors move to get out of the electronically managed market. The Security and Exchange Commission reports a "pattern of institutional investment manipulation." Public anxiety and anger concerning the integrity of the nation's financial system mount giving rise to a major perception management problem for US political leaders. In

information warfare, the secondary effects are likely to be more important than an attack's immediate damage.

Perception Management is the Common Thread in Information Conflicts

From a government leadership perspective, the majority of information age weapons land with at least one foot in the perception management category. Corruption or destruction weapon types are normally targeted against organic essential or infrastructure centers of gravity but clearly their effects are not limited to these categories. Perception management issues are particularly critical for leaders because they must be able to address the people's anxieties and concerns. Information attacks will generate such questions from the public as:

- What other systems are vulnerable?
- How big is this problem?
- Why has the government not provided greater security?
- Who is responsible for defending against these attacks?
- What are they doing about it?

Information age media compounds the problem. Consider, for example, public reaction to the President or telecommunications Chief Executive Officers after a public switch network, which serves as a transfer point for thousands of communications each day, fails for a third time. When answers remain scarce, public support for senior leadership is sure to wane. The degree of skill demonstrated in handling these issues determines the ability of government leadership to maintain the fragile link between Clausewitz' government leadership and their people. Unless leaders can answer the people's questions satisfactorily, the danger exists that public pressure will

force national security policy changes that may not be in the nation's best interest.

1. United States, Dept. of Defense, Defense Science Board, 28, 51.

2. United States, Congress, Office of Technology Assessment, Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage, (Washington: GPO, Jun. 1990) 1, 2.

3. United States, National Communication System, An Assessment of the Risk to the Security of Public Networks, (Washington: National Communications System, Dec. 1995) ES-1.

4. International Energy Agency, The International Energy Agency Natural Gas Security Study, (Paris: Organization for Economic Cooperation and Development/International Energy Agency, 1995) 183.

5. Warren Christopher, et al, American Hostages in Iran: The Conduct of a Crises, (New Haven: Yale University Press, 1985) 180.

CHAPTER 6: Conclusions

Rethinking Grand Strategy Requires Vision and Public Debate

The emerging "information age" has brought enormous benefit to the United States. US technological superiority promises to maintain the nation's world leadership well into the next century. However, US reliance upon technology has grown into dependence and that has resulted in a new form of strategic threat aimed at the information systems that control key aspects of its military, economic, and political power.[1] This new strategic threat calls for a rethinking of US grand strategy for information age national security.

Such an effort requires us to rethink our basic national security objectives. We must start with the most important question: What do we want to achieve? In the United States, the answer to that question requires both vision and national debate. The vision that is beginning to emerge is information assurance. Simply put, we seek to promote the confidentiality, integrity and availability of our information and the reliability of our information systems. It is a vision, however, that given the present state of technology does not permit universal attainment. The US government alone cannot provide security for the entire information spectrum nor for the interconnected systems that run the nation's critical assets. Therefore, we must abandon the idea of universal protection in favor of selective defense. We must focus on those systems deemed essential to the nation's health.

The impossibility of providing universal protection requires the setting of priorities that in turn requires an assessment of information's value and its vulnerabilities. That gives rise to public debate. Given the pluralistic nature of our society, the equities of competing interests in the

information infrastructure and the pervasiveness of information technology, the debate is likely to be lengthy and vigorous. The Department of Defense, as the nation's principal defender, can and should play a leading role in this discussion, but it cannot dictate the outcome. The problem is national in character and the debate must push past government and military discussions until a public consensus emerges that balances the need for government security and personal protection with US Constitutional guarantees and American notions of individual liberty.

A Theme for US Defensive Grand Strategy

The strategic framework we have constructed suggests information assurance should be the theme for US defensive grand strategy. The protection of the information and information systems that are critical to US strategic centers of gravity against destruction, corruption, and perception management weapons must become the catalyst for cooperation between government and civilian entities and the driving force behind the development of new national security policies. Just as "containment" unified national policies and provided a framework for meeting the Soviet strategic threat, so must information assurance provide the basis for a unified response to meet the strategic information threat.

A Pluralistic Framework for the Exercise of Power is Needed

The hard nut to crack in an information age democracy is defining a legitimate role for government that promotes the nation's security while protecting its constitutional guarantees and individual liberties. The purpose of our Constitution is "to provide for the common defense, promote the general welfare and secure the blessings of liberty to ourselves and our posterity."

The genius of the American political system is that it has based its institutions firmly on the concept of division of authority and separation of powers. No one governmental entity has been permitted to amass power to the exclusion of other governmental entities that may reflect different points of view or represent other constituencies. In the final analysis, we are a nation of divergent and sometimes competing interests that relies upon the principle of shared authority to keep the exercise of governmental power in balance. Given the pervasiveness of information technology and its importance throughout the political, military, economic and social fabric of American life, proposals to defend against the information threat by abandoning this principle of shared authority in favor of concentrating power will likely meet overwhelming opposition from the body politic. The nation is not, however, without experience in creating frameworks that recognize differing viewpoints and different constituencies while exercising legitimate governmental powers in furtherance of national security.

Executive Orders 12656, 12919, 12148 and 12472 comprise the legal basis for preparation of national security emergency preparedness plans, the purpose of which are to ensure the continuity of government, at every level, in the event of a national security emergency.[2] A product of the nuclear age, in general terms, these orders instruct various designated executive department heads to identify functions within their areas of respective interest that would have to be performed during national emergencies and to develop the plans and capabilities to do so. They are a formula for protection of the nation's most critical assets in the event of a national crisis. The Secretary of Agriculture, for example, plans for resources preparedness with respect to food resources and food resource facilities; the Secretary of Energy does the same with respect to all forms of energy; the Secretary of Health and Human Services looks after the nation's health

resources, etc.[3] They are a useful precedent in planning to defend against the information threat because they demonstrate how to divide and allocate authority and resources among various agencies representing different constituencies and different sectors of the economy in furtherance of national security.

The challenge of the information strategic threat is a national challenge. The military alone cannot defend against it. Arguably, neither can any other single entity of national government. What is needed is a national entity, a National Information Assurance Council (NIAC), chaired by the Vice-President and composed of permanent representatives from each executive department agency that attends to a portion of the civilian infrastructure deemed vital to national security. The council's charter must be strategic in scope and focus on making national policy recommendations to the President aimed at bringing about a vision of information assurance based upon the confidentiality, integrity, availability, and reliability of our information and information systems. It must be able to allocate finite resources, assess risks, fix responsibility and perform emergency preparedness planning to promote information assurance. Its members must be free to focus on national information assurance matters while at the same time representing their respective constituencies in the process of policy formulation. Since hostile competitors will most likely attack those critical private sector system essentials that will cause the greatest disruption among the civilian population, the council must recognize that defensive information warfare encompasses a much broader spectrum of activities than just protecting friendly command and control systems or vital industrial resources from the threat of hostile information attacks. To be effective, its defensive planning must include measures to defend high value, private sector information and information systems. The council must be

linked to the President's National Security Telecommunications Advisory Committee and to other similar committees representing priority areas for protection. This linkage will help ensure that private sector concerns are brought to the table. In addition, the presence of representatives from the agencies representing these constituencies will help guarantee that private sector commercial needs are not subsumed by the quest for ever greater security.

A Single Agency Executive Agent for Information Assurance is Contraindicated

The nature of conflict has not changed. Warfare's purpose continues to be the coercion of an adversary "to fulfill our will."[4] In this respect, warfare in the information age promises to be no different.[5]

The Department of Defense is charged with defending the nation and should play a leading role in the discussions concerning how to defend in the information dimension of warfare. It has developed the planning expertise, institutions, and human resources to do so. The appearance of new methods and concepts that competitors might seek to attack targets within the United States does not transform conflict in the information dimension into something other than strategic warfare. Its characteristics remain the same: in this case, to force US compliance with a hostile competitor's objectives.

DoD, however, has neither the organizational breadth nor the jurisdictional authority to serve as the lead agency in formulating grand strategy to defend the United States against the information threat. At present, the military services are focusing on their respective pieces of "information dominance." These efforts represent a wartime subset of an information assurance national security grand strategy. While they are important, they are only a part of the total

information assurance need and no matter how well they are developed, they will fall short of a national defense because they do not protect vulnerable information assets in the civilian infrastructure upon which DoD relies.

Neither is the Department of Justice an appropriate lead executive agency as some have advocated. To place responsibility for the nation's defense against the information threat into the hands of the Justice Department commits it to an organization with limited institutional and historical skills in national defense planning, with comparatively limited jurisdiction and experience in world-wide operations and with limited capability to respond externally to structured threats. In addition, as an agency engaged in domestic law enforcement activity, Justice faces a built-in conflict of interest whenever national defense precautions include the official monitoring of private sector security practices and confidential information. This is an important, perhaps crucial, consideration in winning private sector support for national information assurance policies.

Priorities for Protection within US Strategic Centers of Gravity

Our strategic framework suggests the United States must prepare itself to defend both private sector and government information systems. Universal protection is not attainable, nor do we believe it is necessary. A large majority of the material within the information hierarchy of available data, information, knowledge, and wisdom is not vital to national security. Likewise, all of the hardware that forms information systems and networks that make up the civilian information infrastructure does not require protection. In each case, only a small portion of the total amount of information available or number of information systems in operation must be

secured against external forces that would seek to manipulate them. In the case of information itself, the existing paradigm seeks to protect official US Government classified information. That model is clearly outdated and must be revised to include, at a minimum, information that runs sectors of the economy we have labeled system essentials (figure 6-1). With respect to information systems, more and more attention is being paid to the vulnerability of the Public Switched Network (PSN), the critical nodes within the telecommunications industry that route message traffic. Clearly the PSNs must be placed high on any list of information systems to be guarded against tampering.

Within the nation's strategic centers of gravity, information and information hardware that control those systems we have categorized as system essentials offer the most lucrative information targets for competitors as their disruption may cause massive unrest among the civilian population and thereby generate significant political pressures upon the nation's political leaders. We believe priority must be given to these for protection. In addition, within the strategic centers associated with government, i.e., leaders and the defense mechanism, those systems that permit command and control and employment of military forces must also be protected. We believe the balance of information and information systems should be left to the private and commercial sectors.

Leaders	System Ess	Infrastructure	Population	Def Mech
Command &Control Networks	Telecommunications Electric power Gas/oil pipelines Federal Inter-bank transfers	Transportation dispatch systems		Communications networks Logs/Pers Databases Transport. Mgt. systems

(Fig. 6-1) Priorities for protection.

Defending Against Physical Destruction of Information Systems

EO 12656, that assigns certain national security emergency response preparedness (NSERP) activities to the Department of Defense, specifically identifies technological emergencies as an example of a national security crisis requiring DoD's response. Sec. 204 requires the Secretary to:

> Identify facilities and resources, both government and private, essential to the national defense and national welfare, and assess their vulnerabilities and develop strategies, plans, and programs to provide for the security of such facilities and resources, and to avoid or minimize disruptions of essential services during any national security emergency.[6]

Originally designed to ensure the continuity of government in the event of a nuclear war, Sec. 204 nevertheless provides the legal basis for the Secretary to begin planning for the protection of critical US public and private information systems from physical attack. DoD's NSERP planning should be modified to provide physical protection not only for industrial facilities and resources that are deemed critical to the mobilization and employment of military forces but also for key network switching and control systems that manage areas within our strategic centers of gravity designated for priority protection (figure 6-1). Nomination of such areas from outside DoD should be made by representatives on the National Information Advisory Council.

Defending Against Corruption of Information Systems

The threat to US information systems from corruption weapons is a clear and present danger that demands immediate attention. Unfortunately, it is also a threat that requires long term as well as short term solutions. Long term solutions require the establishment of national

institutions with broad charters that cross traditional bureaucratic boundaries, such as NIAC, and vigorous national debate concerning the proper measure of government involvement in something as pervasive in American life as information management. Short term solutions are primarily within DoD and should be pursued immediately.

Both the government and the private sector have had experience with taxonomies that are useful in fashioning separate but complementary responses to the information threat. With respect to the government, institutions existing within the public health sector, particularly the Center for Disease Control, appear to be applicable. In the private sector, national testing organizations such as the National Underwriter's Laboratory provide useful designs for reference.

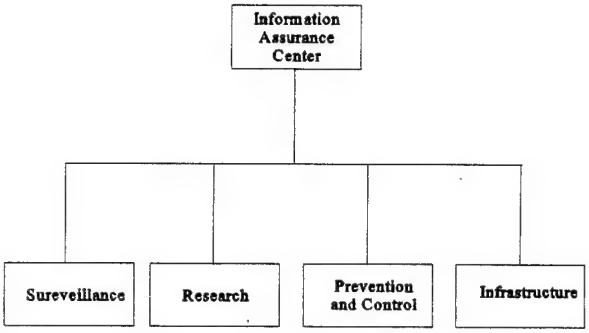
Use of the term "virus" for software programs that surreptitiously enter computers and attack their internal operating systems is an apt metaphor. The characteristics of information conflict, in many respects, are very similar to those of infectious diseases. Anyone or anything can be an infectious disease carrier. New disease strains can circumvent or overcome prepared defenses. Disease carriers are hard to trace, and infectious diseases can pass through multiple carriers. The same is true of information conflicts.[7]

Just as it took the federal government to marshal the resources and expertise necessary to mount an effective counterattack against the spread of infectious diseases, so should the federal government create the national institutions and processes necessary to blunt and roll back the onslaught of electronic diseases. The spread of electronic infections through networked technology, as we have seen, places the nation's well being clearly at risk. As the entity responsible for information assurance, NIAC should establish a separate information assurance center, patterned after the Center for Disease Control, to combat the strategic threat posed by the

outbreak of electronic epidemics.[8]

NIAC's information assurance center should be resourced and empowered to carry out four functions: surveillance, research, prevention and control and infrastructure (fig. 6-2).[9]

The surveillance function should monitor the outbreak of electronic infections both within the United States and internationally. The history of public health teaches that suppression of infectious diseases must be preceded by an understanding of their behavior and the methods of their transmission.[10] The same is equally true of information corruption weapons. Within the United States, reporting criteria must be implemented to ensure the new information assurance center is properly notified of potentially contagious electronically induced disruptions of service within designated priority areas for protection and/or of the employment of certain types of information corruption weapons.



(Fig. 6-2) Information Assurance Center.

Research should focus on how hardware, software and human behavioral factors influence the emergence or prevention of information corruption; the effectiveness and economic benefit of strategies to prevent corruption of information systems; and the development of improved techniques for identifying emerging technologies that promote or restrict the spread of electronic infections. An added function is to establish programs to promote effective partnerships with public agencies, universities and private industry to support research in surveillance, and the prevention and control of technological attacks against information systems.

Prevention and control deals with public education and with the implementation of measures designed to prevent or contain the outbreak of infectious information attacks. This function includes the development and dissemination of information to the public that informs and educates about the nature, methods of transmission and pathologies of information corruption software. It also contains rapid response teams to investigate and contain massive disruptions of systems that control priority areas for protection.

The infrastructure function looks to development of a national network of professional and support personnel to understand, monitor and control electronic infections. It will provide training in reporting criteria, diagnostic evaluation and surveillance of new and re-emerging threats.

National security strategists must remember that the US information infrastructure is a creature of the private sector. It is being built, owned and operated by private citizens and private commercial concerns. In addition, the products and services that are used to process and store information over its networks are produced primarily by private sector companies. Although the federal government has an important role to play in the infrastructure's continued growth and development, it does not presently, and should not, occupy the position of an information infrastructure regulator under the mantra of national security. There is a need, however, for improvement in the security of private sector systems lest sectors of the economy serving large segments of the population, as well as the government, experience significant disruptions. The private sector must accomplish this task.

The National Security Telecommunications Advisory Committee (NSTAC) has proposed the creation of a privately funded Security Center of Excellence (SCOE) to assess the security of

origination, termination, intermediate, and transport systems and facilities within the Public Switched Network (PSN).[11] The center would serve as a sort of National Underwriter's Laboratory for information systems. The President, as well as DoD and other agencies interested in information assurance, should support and encourage this initiative.

The SCOE will perform three functions: 1) review and adopt security evaluation standards, 2) develop and promulgate methodologies for evaluating and rating security products and systems, and 3) enhance communications between industry, government, and the public on the need for implementation of information assurance measures.[12] An entity that performs these functions, in an environment free of bias and conflict-of-interest will serve a number of useful purposes.

First, it will provide standards and methodologies that testing laboratories can use to evaluate the security of existing products and of those being introduced into the market. Such testing, impossible in the absence of recognized industry standards, will provide a means of measuring product and system trustworthiness and integrity. The introduction of standards where none now exist will gradually produce a marketplace that generally reflects the level of security promulgated as being usual and customary within the particular industry being examined. The result is an overall improvement of security within the information infrastructure.

Second, the introduction of industry wide security standards limits the liability of companies that adhere to them. A company that implements security measures commensurate with those recommended by the SCOE will most likely have met the reasonably prudent person standard that results in the avoidance of liability in civil litigation. The converse, of course, is that companies ignoring such standards are likely to find themselves the targets of civil lawsuits.

Hence, the existence of standards performs an additional function of regulating the industry by exposing those who do not follow them to the risk of serious financial hardship and likely loss of business.

Finally, publication of security standards can be expected to help stimulate public interest in and demand for products and services that provide a greater measure of information assurance, balancing protection and privacy. NSTAC predicts that upon publication of such standards the security consulting industry will move to promote and implement them resulting in their rapid adoption throughout the infrastructure.[13] The end result will be a more reliable PSN.

Defending Against Perception Management

"Our influence will increasingly be defined more by the quality of our ideas, values, and leadership...than by the predominance of our military capabilities."[14] In an age where information is instantly disseminated, ideas count as never before. Determined adversaries will use perception management techniques to manipulate ideas to push US public opinion toward positions that favor their own and to undermine public confidence in national leaders who oppose them.

Above all else, US policy makers must communicate the goals and objectives of national security policies clearly and simply. Such communication promotes understanding by the widest possible audience and helps to generate support for the commitment of US forces in furtherance of national security objectives. It also helps to ensure that the nation's security policies conform with America's declared ideals and beliefs. If otherwise, the images generated by adversaries will quickly point out the dichotomy and predispose the American population to the employment of other perception management techniques.

The importance of ideas in a era of instant communications means that the US must be capable of responding to media demands for instantaneous reactions to world events with positive real time images of its own in support of national policies. The government's knowledge machinery that supports the President and senior government leaders must be able to prepare both information and more importantly compelling television video as quickly as CNN can present its news and analysis. The objective must not be to point the television spotlight elsewhere, dim it or switch it off, but rather to challenge it for accuracy and context with images that counteract distortions and half-truths.

Determining the adequacy of these defensive countermeasures will require new measures of effectiveness for grand strategy. We presently have no definable method to assess the criticality of individual pieces of the infrastructure or the benefits of protecting or the risks of not protecting them. Without these measuring tools, and the sound logic needed to produce them, the effort to build adequate defensive countermeasures will lag behind offensive capabilities.

1. Kenneth E. deGraffenreid and Michelle Van Cleave, "Information Assurance and the Future of the NCS," draft, (Fairfax, VA: National Security Research, Inc., 12 May 1995) 5-6.

2. "Executive Order no. 12148, Federal Emergency Management," 44 Federal Register 43239, 20 July 1979; "Executive Order no. 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions," , 49 Federal Register 13471, 3 Apr. 1984; "Executive Order no.12656, Assignment of Emergency Preparedness Responsibilities," 53 Federal Register 226, 18 Nov. 1988; "Executive Order no. 12919, National Defense Industrial Resources Preparedness," 59 Federal Register 29525, 3 Jun 1994.

3. "Executive Order no. 12919, National Defense Industrial Resources Preparedness," Federal Register, Sec. 201.

4. Clausewitz, 89.

5. David S. Alberts, Defensive Information War: Problem Formulation and Solution Approach, (Washington: National Defense University, 17 January 1996) 5.

6. "Executive Order no.12656, Assignment of Emergency Preparedness Responsibilities," Federal Register, sec. 226.

7. Paul A. Strassmann, "Defending the Military Infrastructure," address, National Defense University, Washington, 11 Mar. 1996.

8. Paul A. Strassmann, "Risk-Free Access Into the Global Information Infrastructure Via Anonymous Re-Mailers," Symposium on the Global Information Infrastructure, Kennedy School of Government, Harvard University, 28-30 Jan. 1996. The metaphor of infectious diseases and the concept of a Center for Disease Control-like response within DoD is the brainchild of Mr.Strassmann.

9. The functions of the proposed DoD information assurance center were adapted from Addressing Emerging Infectious Disease Threats: A Prevention Strategy for the United States, (Atlanta: Center for Disease Control and Prevention, Apr. 1994).

10. Strassmann, "Risk-Free Access Into the Global Information Infrastructure Via Anonymous Re-Mailers."

11. National Security Telecommunications Advisory Committee (NSTAC), Report to NSTAC XVIII, (Washington: National Information Infrastructure Task Force, Feb. 1996) B-3.

12. NSTAC, B-7.

13. NSTAC, B-8.

14. United States, The White House, National Security Strategy of the United States, (Washington: GPO, August 1991) 14.

Chapter 7: Recommendation...A Strategic Plan

> We insure against loss of life, against loss of money, against destruction by fire or storm, and, in fact, against the loss of possession or attribute which we deem of value...The country or state is the highest form of insurance policy, and it is underwritten by a policy of national defense...
>
> John Weeks, Secretary of War, 1923.

A Strategic Plan for National Security

Our vision provides a focus for long term planning, and the mission establishes our day-to-day responsibilities. Mission related decisions are made not only to accomplish short term objectives, but to achieve the vision. "Vision focused and mission driven" define our boundaries. The goals of this plan provide priorities as we move forward to achieve its vision.

The momentum of recent efforts to address the issue of information assurance positions the US to make great progress in the years ahead. However, we must keep in mind two points: *First*, it will take time, patience and persistence to refine this plan and to develop the relationships necessary to achieve its goals. *Second*, we need to start now.

The course is set.

Vision: Information Assurance for the 21st Century

- A national commitment that secures confidentiality, integrity and availability of information and the reliability of information systems.

- A national consensus balancing government security and personal protection with US Constitutional guarantees and American notions of individual liberties.

Mission: Plan, Assess, Coordinate and Conduct Activities to Achieve Information Assurance

- Identify and assess vulnerable information nodes within priority areas for protection.
- Identify and assess the strategic threat to US information and information systems.
- Develop proactive prevention and control measures that detect, deflect and defeat intrusions into, or structured information attacks upon, priority areas for protection.
- Develop the capability to execute those plans.
- Develop national institutions that build US Government and private sector equities in information assurance.

Goals: National Imperatives

We must produce a national security grand strategy that includes defending the nation's information infrastructure because the nation's viability - political freedom, economic identity and military power - now depends upon it. Achieving this objective will require educating the American people to understand that national security is not the sole responsibility of the DoD and that national security crosses traditional economic, political and military boundaries. We must seek to promote vigorous public debate about the role of government in information assurance to build a strong national consensus as to how we will achieve our goals. The debate must clearly include an assessment of the need for intelligence sharing among all the national security stakeholders. Painful choices may have to be made to reshape national defense policy in the information age.

- Lead a vigorous public debate. The information age presents security risks that are economic and political, and not solely military in nature. These threats must be made known to the American people. As a first step in building public support for new national security priorities that are becoming more complicated daily.

Government agencies and the commercial sector must find common ground to underwrite a national commitment to information assurance.

- Unify a government/private sector response to protect the confidentiality, integrity, availability, and reliability of US information and information systems against the strategic information threat. Replace "containment" with "information assurance" as the vision upon which US national security grand strategy is based.

- Abandon the idea of universal protection in the information dimension in favor of selective defense that focuses on both government and private sector information and information systems deemed critical to national security.

- Give Information assurance priority for protection to the system essentials strategic center of gravity and, within it, specifically to telecommunications switches, electric power distribution mechanisms, gas and oil pipeline distribution mechanisms, inter-bank transfer mechanisms and transportation dispatch systems. Within the defense mechanism center of gravity, communications networks, logistics and personnel databases and transportation management systems must also be protected.

- Establish a National Information Assurance Council (NIAC) to make national security policy recommendations to the President aimed at bringing about our national security vision of information assurance.

- Establish an Information Assurance Center, patterned after the Center for Disease Control, and answerable to NIAC to perform surveillance, research, prevention and control and infrastructure functions within the information assurance mission.

- Expand US National Security Emergency Response Preparedness (NSERP) planning to include physical protection for key network switching and control systems that manage areas within our strategic centers of gravity designated for priority protection.

- Encourage the President and Congress to support the National Security Telecommunications Advisory Council (NSTAC) efforts to establish a Security Center of Excellence and expand the NSTAC concept by creating similar committees in areas designated for priority protection.

- The President's knowledge machinery should be enhanced to provide timely responses to the media's demand for immediate reactions to national security events and to provide accuracy and context to media reporting.

Goals: DoD Imperatives

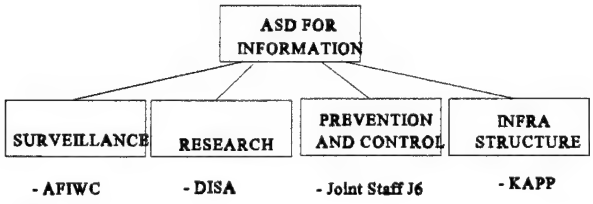
The US military must play a leading role in devising this strategy but cannot do it alone. DoD must be included in any strategy for defending military and commercial information systems because our national defense depends upon it and because ability to bring combat power to bear in support of national objectives relies on its ability to deploy and sustain American forces. In the short term, DoD must act to resolve its own information assurance requirements, and to understand that national security in the information age is more than information dominance.

- SecDef submit information assurance and its information age strategic implications as part of the next National Security Strategy.

- Direct CJCS to promulgate a new National Military Strategy that addresses the information assurance vision and its wartime subset of information dominance. As "containment" carried significant grand strategy meaning throughout the Cold War, so a new policy of "information assurance" must be understood at the grand strategy level and as a part of the National Security Strategy.

- Retitle the Assistant Secretary of Defense for C3I as the Assistant Secretary of Defense for Information. Expand the position's focus beyond C3I to incorporate such areas as CONUS defense against information attacks.

- Assemble a DoD organization for defense information assurance. Use core competencies already available within DoD to replicate the health taxonomy used for national information assurance. Figure 7-1 displays some possibilities.



(Fig. 7-1) Sample military information assurance hierarch

- Recommend a change to the Unified Command Plan. Designate CONUS as an area of responsibility (AOR): task CINCUSACOM or CINCSTRATCOM with a CONUS defensive information warfare responsibility. Include an aggressive, quantitative modeling and simulation effort for defensive information warfare.

- Direct CINCUSACOM to restructure the Key Asset Protection Program by: (1) Assessing key asset vulnerabilities to corruption information weapons as well as physical destruction weapons; (2) Adding system essential priority areas for protection to the Key Asset List; (3) Expand the KAPP evaluation and review board to incorporate experts from appropriate fields; (4) Expand planning and training to incorporate new Key Asset List physical protection requirements; (5) Thoroughly document all actions needed to address information vulnerabilities.

- Merge KAPP analysis with current vulnerability net assessments to identify the potential repercussions of a structured information attack upon system essential assets. Assume aggressive, quantitative modeling and simulation effort for defensive information warfare. Recommend higher levels of information assurance for national security.

- Direct a review of operational plans for the Land Defense of CONUS to incorporate potential impacts resulting from information attacks and degradations to the information infrastructure. Include aggressive modeling and simulation as part of the OPLAN review.

- Direct a review of defense contingency plans to ensure they incorporate the full breadth of information warfare options and brief the NSC on these new options as well as the potential for their use against the US.

Appendix A: Anecdotal Evidence

The following incidents are not provided to suggest chaos on the information highway, but rather that, in the hands of malevolent actors, the capability already exists to cause significant disruption to information systems vital to US national security. While assertions of a national disaster may be somewhat premature, anecdotal evidence suggests the US is already vulnerable to information attacks. In recent years, unknown intruders have penetrated US telecommunications carriers, Internet service providers, many international post, telegraph and telephone entities and a wide variety of end user systems.

Wired Magazine names the top ten infrastructure targets including the Culpeper PSN that handles federal funds transfers and WWMCCS.[1] Additional targets include: Satellite dishes associated with GPS (and time synchronization for precision munitions), satellite dishes associated with national intelligence and defense activities (the "Big Blue Cube" in Mountain View, California and the National Photographic Intelligence Center), the Internet, computer directed telephone and power distribution transfer points (including the Alaskan Pipeline), and computers associated with major banking and financial institutions. Targets of intrusion include:

- physical attacks on infrastructure components such as computers, communications, software, data cables and control process; infrastructure support such as buildings, power and environmental control units; and attacks or subversion of operating and support personnel.
- Logic attacks on infrastructure components; attacks on computer controlled environmental control units; and attacks on data (destruction or corruption).
- Combined logic and physical attacks to mask each other[2]

Financial Losses

In 1991, the FBI Director said "as much as $5 billion a year" was lost by American

companies due to computer related crime.[3] By 1995, the Dallas Morning News reported "$10 billion worth of data" was stolen annually in the US from "on-line thieves."[4] The real threat to American interests lies in the ability of criminals to infiltrate and destroy US financial and information systems. Hackers who pioneered breaking into computer systems for fun are selling their abilities to criminals.

- The New York Times reported in August 1995 that a $10 million computer fraud case had been uncovered involving a 34 year old Russian and accomplices who moved money from his keyboard in St. Petersburg, Russia, via wire transfers from Citibank accounts in Argentina and Indonesia. In response, a bank spokesperson ensured that all but $400,000 of the cash had been recovered and offered some perspective to the problem. She said, "We move half a trillion dollars a day through the payment system...compare that to $400,000...we think we have the right level of security." In major bank frauds involving electronic funds transfers, first detection is normally the bank audit, usually several months after the incident.[5] [6]

- During the Soviet era, criminal groups and the black market functioned as an extension of the Communist Party and the KGB. These criminal organizations outlived the state which fostered them. There are roughly 5,700 organized crime groups in Russia. Of these, 200 are large sophisticated criminal organizations engaged in activity throughout the former Soviet Union and in 29 other countries. These criminal groups are also targeting the financial sector. Banks have become a particular target for money laundering schemes. Links have been forged between Russian and Italian organized crime groups to move money through the Russian banking system.[7]

- A software glitch was the cause of a $70,000,000 government loss due to overpayment by the Health Care Financing Administration. About 100 health care organizations received overpayment--the largest was $19,000,000 - due to a software problem that failed to crosscheck Medicaid charges against people eligible for Medicaid.[8]

- In 1991, a US car manufacturer lost approximately $500 million when a hacker broke into its network and stole future auto designs which ended up in the hands of its competitors.[9]

- A 1994 survey of business losses due to information security problems had 1,271 respondents of which over 50% claimed financial losses due to information security issues. 17% had losses up to $250,000; 3% had losses between $250,000 and $1,000,000; and 17 reported losses in excess of $1,000,000. Biggest concern is integrity and availability of information.[10]

- In October, 1992, IRS internal auditors identified 368 employees who had used the IRS's Integrated Data Retrieval System without management knowledge, for non-business purposes. Some of these employees had used the system to issue fraudulent refunds or browse taxpayer accounts that were unrelated to their work.[11] In April 1996 a former IRS worker pleaded guilty to federal charges for illegally tapping into more than 150 confidential tax records.[12]

- Authorized users of the FBI's National Crime Information Center misused the network's information by gaining access to files to determine if friends, neighbors, or relatives had criminal records or inquire about backgrounds for political purposes.[13]

- NCS says there is significant evidence of insiders selling information to information brokers, industrial spies, criminal organizations, and intelligence services. These insiders, with full access to their respective information files, have provided data on unpublished telephone numbers, toll records, credit reports, and other personal data. The FBI reported that criminal organizations have gained access to the National Crime Information Center records primarily through the use of compromised employees. In December 1991, 18 Social Security Administration employees were indicted for sale of confidential information.[14]

- In August 1992, a computer systems administrator for a defense contractor was told of a pending layoff. The employee set up a malicious code to activate after his departure. He hoped that the company would hire him back to reconstruct databases after the logic bomb functioned. His attempt was discovered before he left and he later pleaded guilty to the charge. If the malicious code had functioned, substantial data on the development of military missile systems would have been destroyed and required months to reprogram the computer system.[15]

Telecommunications Targets

The public telecommunications networks are a critical part of the DII/NII (95 percent of DoD telecommunications is provided by public networks and operated by common carriers) but lack the assurance features needed for military use.[16] [17] There have been multiple incidents (mostly accidental) in which the assurance designs were unable to meet the challenge of accidental errors and omissions. Most commercial networks have little or no coverage against intentional disruption and commonly fail from either software errors or mischievous or malicious attacks. Additionally, telephone switching errors must be repaired within 1.5 seconds or the circuit errors

passing through the network will propagate, causing major disruption. An attacker needs to disrupt only 2 of the 9 PSN sites for 1.5 seconds to cause a cascading effect.[18]

- In 1991, a near total shutdown of telephone service in the Baltimore-Washington area was caused by a 3 bit coding error where a "d" was replaced by a "6" in one byte of a software upgrade causing disruption of ATT long distance service to millions of customers for over four hours. None of the few broad phone outages that have occurred has been shown to be caused by anything other than faulty software, though the signalling systems have been under hacker attack affecting service to customers. The point made is that though there have been no catastrophic failures, the potential exists.[19]

- On September 17, 1991, AT & T announced a "power failure" had caused two major switches to fail. This failure forced the shutdown of major airports that rely on ground-based telephone lines for both voice and data communications for air traffic control in the New York City, Boston and Washington Air Route Traffic Control Centers. The result was disruption of the civil aviation industry into the Northeast US for days, resulting in flight delays across the nation.[20]

- In 1993, FAA computer system failures (cause unknown) delayed regional traffic for 90 minutes and an FAA weather computer failed for 12 hours due to a time-activated logic bomb.[21]

- Other Phone System Failures - A highway crew digging post holes disrupted coast to coast calls by cutting a MCI fiber-optic cable. A similar incident in New Jersey cut 60% of the calls in and out of Manhattan for eight hours. In this incident the New York Mercantile Exchange and the Commodity Exchange had to shut down operations.[22]

- Electronic intruders have shown the abilities to service control points, service provisioning systems, cross-connect systems, modify user services, forward calls, modify service class on circuit, turn off billing on specific circuits, routing tables, and service descriptions. Scott Maverick compromised 911 services in 1992. He was arrested for tampering with these systems in Virginia, Maryland, and New Jersey. Maverick said his intent was to infect the 911 computer with a virus to cause havoc. "Significant degradation of service for 911 systems is possible if they are targeted by electronic intruders."[23]

- An April 1991 effort for a complete computer and telephone system invasion was the most comprehensive, coordinated attack on the PSN to date. Kevin Poulson pleaded guilty to all but one of the following counts: compromised an ongoing law enforcement investigation; identified law enforcement run businesses and law enforcement wiretaps; intruded on the Local Exchange Carrier (LEC) service provisioning system numerous times (allegedly more than 40); modified existing telephone services, added new telephone services (some without billing), forwarded calls to other numbers, and dual-provisioned telephone lines; intruded on LEC maintenance/test systems to electronically monitor

telephone conversations; intruded on LEC databases and obtained telephone numbers (some unlisted), street addresses, customer names, and other sensitive data; physically broke into carrier offices, and stole equipment, software, identification badges, and other material; sold sensitive data obtained from LEC databases, and illegally established or modified telephone services for other individuals; manufactured false identification, including telephone company identification badges and drivers licenses, intruded on other computer systems for profit, including the California DMV, credit bureaus, and an Air Force computer network; illegally possessed classified documents (the one count he pleads not guilty on); laundered money. Although Poulsen did not attack PSN networks he did manipulate the system to his own ends and to his own personal profit.[24]

Viruses

Computer viruses can disrupt tactical operations, trends in military electronics systems make them more vulnerable. "There is a concerted effort in the former Soviet client states to perfect computer crimes. There are universities...that teach how to create more effective viruses."[25] There is limited direct evidence and substantial indirect evidence that disruption technology exists in many nations: former USSR, US, Bulgaria, Poland, Germany, Netherlands, Italy, Canada, UK, Taiwan, Sweden, Israel, Spain and Australia (among others). It is clear that from computer virus information alone that many countries of security interest of the US have knowledge and technology to corrupt computer and network data and disrupt operations, among them: India, Taiwan, Republic of Korea, China, Japan and South Africa.

- A November 1988 virus (Morris Worm), placed on the Internet by a college student infected 6000 host computers in less than two hours and cost between $100,000 and $10 million to clean up, affecting network links between MIT, University of California, Sandia Labs, Lawrence Livermore Labs, Los Alamos National Research Lab, and others.[26] [27]

- A Christmas card message sent over BitNet, a global academic network, landed in 2,800 machines in 5 minutes, including IBM's internal network. It took only five hours for the benign virus to spread 500,000 infections worldwide, forcing IBM to take the network down for several hours to accomplish repairs.[28]

- In 1992, Novell released a virus to thousands of customers in shrink wrapped software due to a procedural error. The master disk was infected by a virus due to mishandling and failure to adhere to company policy during transportation to the disk duplication center.[29]

- Multiple books have been written on software viruses, including tutorials on how to write viruses aimed at military use software. An interactive CD-ROM movie "Soft Kill" released in 1993 illustrates information warfare against the United States. It details corrupting time standards, affecting precision guided weapon targeting and also targeting long distance telephone switches. [30] Tom Clancy's book "Debt of Honor" has a central theme of crippling information warfare attacks on the United States by means of viruses, worms and logic bombs, HERF guns, and EMP bombs. The author's examples are not considered as malicious or as subtle as a real attack by experts would be.

Hackers

Hackers are the first group to learn of US vulnerabilities and are quick to share the information. Hacker magazines routinely tell hackers how to build and plant viruses, break into computer networks through access to telecom circuits, and gain entry to government networks. The Defense Information Systems Agency (DISA) have detected unknown intruders gathering Internet passwords through "sniffer" programs. In one 1994 observation period they estimated the number of captured passwords "at a million or more, potentially threatening all the host computers on the Internet and their users."[31] In another test, DISA conducted a test of logistics and medical network vulnerabilities in which they attacked 9,000 computers, successfully hacked 88% and only 4% of successful attacks were detected.[32] Network administrators at the Air Force Information Warfare Center said they could crack 70% of the passwords on their UNIX network with tools resembling those now being used by Internet hackers.[33]

- NASA's information technology security program manager, Rick Carr, said there are about 1,000 network break-in attempts a month, nearly fourfold over the last two to three years. Since November of last year, NASA documented six "high impact" attacks that have compromised sensitive or classified information. Losses were put at more than $250,000 per incident. Intrusions have resulted in theft and damage of research data.[34]

- Computer hackers infiltrated General Electric's computers, gaining access to research and proprietary information. The intruders managed to penetrate robust security barriers, known as firewalls. The hackers had also obtained passwords of workers who were using

GE computers to connect to more than a dozen Internet computers. The GE spokeswoman said "we just know we were compromised."[35]

- An MCI employee was charged with stealing 100,000 calling card numbers and used them to place $50,000,000 worth of fraudulent calls. The employee wrote software to capture card numbers from various carriers that used MCI's switching equipment. He sent the captured numbers to an international hacker ring.[36]

- On January 13, 1995, the Naval Academy Network had to be shutdown due to password-sniffing software in one-third of its servers. The network is used by faculty, staff and midshipmen. The academy was unable to determine how many passwords were collected or if the intruders had used the network as a launch pad into other DoD or Federal systems.[37]

There are several hacking groups in Europe that keep lists of US military C2, research and logistics computer accounts attained through hundreds of military Internet connections. The list is easily accessible.

- Project RAHAB is the German government's computer espionage program. Beginning in 1988 as an ongoing computer intrusion research effort, its primary focus is on cataloging network addresses and establishing pathways for later use. Its technicians have allegedly accessed computers in Russia, Japan, France, US, Italy, and Britain. [38] [39]

- The Hannover hackers are a European hacking group that have been linked to the KGB. They gained illicit entry to over two dozen classified computer systems (as well as many others that were unclassified), and were caught when a 75 cent billing error was discovered at the Livermore Laboratories in Berkeley, CA. Leader, Markus Hess, was able to acquire "superuser" status on network, surreptitiously stole authorized passwords for later exploitation. He penetrated "Dockmaster" computer security database at the National Computer Security Center, a component of the National Security Agency. The case is rare where state sponsored espionage has been acknowledged. Numerous other intrusions have been noticed and the frequency of intrusions is increasing.[40] [41] [42]

- Shortly after Iraq's invasion of Kuwait in 1990 a large scale effort was launched worldwide to penetrate various sensitive US government and military computers. Although most of the penetrations originated in the Netherlands, an Iraqi intelligence operation against NATO was uncovered at the same time. The Dutch hackers penetrated host computers at Lawrence Livermore laboratories in the US then branched out, penetrating computer systems at 34 DoD sites by weaving their way through university, government, and commercial systems on the Internet. They exploited a security hole in

the Trivial File Transfer Protocol, which allowed users on the Internet to access a file containing encrypted passwords without logging onto the system.[43] The hackers were in a position to sell the gathered intelligence, either directly or indirectly, to Iraqi intelligence.[44] Dutch hackers successfully penetrated US military computer systems at least 34 times between April 1990 and May 1991. Pentagon officials report these same hackers offered to disrupt the US military's deployment to the Middle East in return for payment from Saddam Hussein in the amount of $1 million. Saddam spurned the offer.[45]

- Another case of hacking for possible espionage purposes involved a 16 year old British cracker with the Internet name "Datastream" who cracked into South Korea's nuclear secrets via the Air Development Center at Griffith Air Force Base, New York. He obtained information on North Korea's missile firing sites, aircraft design and US agents in North Korea. Richard Price, a London music student was charged with 12 offenses of unlawfully gaining access to USAF, Lockheed/Martin computers. Following a thirteen month US/UK intelligence agency operation, Price was arrested by UK police. He gained access on at least 69 occasions.[46]

- In 1995-96, an Argentine graduate student in Buenos Aires broke into sensitive US military and NASA files after gaining access through Harvard, UMASS and Northeastern University computers. Julio Ardita breached computer security by obtaining passwords through a sniffer program that he transmitted to Harvard and other sites through the Argentine telephone system, Telecom. After obtaining the password to Telecom, he was able to break into computer systems run by US universities, the US Navy, other US agencies, and other computers in Korea, Mexico, Taiwan, Chile and Brazil.[47] [48]

- USSR succeeded in gaining access to production information on the NATO "Tornado" jet fighter in 1984 by accessing databases of the Messerschmitt-Bolkow-Blohm company in Munich. Soviet computer hacking involved some 2.4% of overall Soviet espionage operations in 1983.[49]

- DST, the French government's electronic data collection program, has a "hot list" of firms targeted for electronic monitoring; including: IBM, Dow Chemical, General Electric, Corning, Texas Instruments, AT&T, GTE, Du Pont, Siemens, Hitachi, Fujitsu, Sony, Bosch, BASF, and Boeing.[50]

- German intelligence agents managed to illegally access hundreds of computers worldwide through NASA's SPAN network. They managed to break into the CERN physics laboratory computer system in Geneva and loaded a damaging Trojan Horse that destroyed software and crashed systems.[51]

- There is growing evidence of the use of electronic intrusion techniques by industrial spies. In a survey of 150 high technology research and development companies, 48 percent said they had been the target of trade secret theft. Kevin Mitnick was arrested and prosecuted

in 1989 for stealing more than $1 million in source code from Digital Equipment Corporation (DEC), modifying it to add "trap doors," and attempting to copy it back to DEC's development computers.[52]

Destruction (Physical Attacks)

The globalized digital information system offers lucrative targets in a terrorist's strategy of destabilizing the socio-political order. The terrorist chooses people as his most effective target, to influence, rather than kill them, by attacking targets that affect the largest number of people, thus attracting publicity. In Japan, terrorists have attacked the computerized control systems for commuter trains, paralyzing major cities for hours. In Italy, the Red Brigade's manifesto specified the destruction of computer systems and installations "for striking at the heart of the state."[53]

- On 10 April 1992, the IRA set off a bomb in the Square Mile of London. Though three people were killed, the intent was not to kill; it was an attack on the financial center of Europe, causing severe effect - electronic, financial and psychological - on the world's business community.[54] There have been five bombs set off in London between 1990 and 1996 to make similar political statements.

- The World Trade Center bombing of February 1993 is another example of physical destruction to make a political statement. The goal was to shut down the New York financial system. There were 6 killed and over 1,000 injured, however, there were no serious systems losses, due to back-up system operation.

- Investigation of the 1995 crash in an isolated portion of Arizona desert revealed a computer monitored safety device had been short-circuited. The system was designed to warn of sequential loose rails but failed to operate because of apparent intentional tampering.

1. SAIC, Planning Considerations for Defensive Information Warfare, 16.

2. SAIC, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2-7.

3. William S. Sessions, "Computer Crimes An Excalating Crime Trend," FBI Law Enforcement Bulletin, Feb. 1991, 12.

4. "Net Profit Or Loss," Security Awareness News, Oct. 1995, 8-10.

5. Saul Hansell, "Citibank Fraud Raises Computer Security Questions", New York Times, 19 Aug. 1995: 31.

6. John Alger, "Information Warfare: Hackers, Crackers, and the Projection of Power", address, Third Tuesday Seminar Series, George Washington University, Washington, 17 Oct. 1995, 1.

7. United States, Senate, Committee on Foreign Relations, Hearings on the Subcommittee on Terrorism, Narcotics, and International Operations, Washington: GPO, 20-21 Apr. 1994, 103-606. Testimony of R. James Woolsey, Director of Central Intelligence.

8. James Smith, "Logic Flaw is the Culprit in Computer Mugging," Government Computer News, 7 Nov. 1994: 12.

9. Schwartau, 116.

10. SAIC, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, B-58.

11. United States, Congress, Office of Technology Assessment, Information Security and Privacy in Network Environments, (Washington: GPO, Sep. 1994) 3.

12. "Former IRS Worker Admits Snooping," Boston Globe, 5 Apr. 1996: 25.

13. United States, Congress, Office of Technology Assessment, 2.

14. United States, National Communications Sytem, 2-13, 2-14.

15. United States, National Communications System, 2-13.

16. Neil Munro, "The Pentagon's New Nightmare: An Electronic Pearl Harbor." Washington Post, 16 Jul. 1995: C.3.

17. SAIC, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2-70.

18. SAIC, Planning Considerations for Defensive Information Warfare, 36, 37.

19. SAIC, Planning Considerations for Defensive Information Warfare, 36, 37.

20. United States, General Accounting Office, Information Superhighway: An Overview of Technology Challenges, (Washington: GAO, 23 Jan. 1995) 36.

21. SAIC, Planning Considerations for Defensive Information Warfare, 37.

22. United States, GAO, Information Superhighway: An Overview of Technology Changes, 37.

23. United States, National Communications System, 4-3, 4-5.

24. United States, National Communications System, 2-9, 2-10.

25. Pat Cooper, "Organized Crime Hackers Jeopardize Security of U.S.," Defense News, 3 Oct. 1994: 18.

26. Elmer-DeWitt, 76.

27. SAIC, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2-7.

28. Haas,18.

29. SAIC, Planning Considerations for Defensive Information Warfare, 37.

30. "Soft Kill" (Interactive CD -ROM) XIPHAS, 1993.

31. United States, Congress, Office of Technology Assessment, 3.

32. Neil Munro, "New Information War Doctrine Poses Risks, Gains," Washington Technology, 9.18, 22 Dec. 1994, 1.

33. Sharon P. McCarthy, "Network Break-ins Reveal the Chinks in Systems Security," Government Computer News, 8 Aug. 1994, 63.

34. Elizabeth Sikorovsky, "Internet Break-ins Compromise Hacker Attack," Federal Computer Week, 19 Dec. 1994, 4.

35. Jared Sandberg, "GE Says Computers Linked to Internet Were Infiltrated," The Wall Street Journal, 28 Nov. 1994: B.5.

36. Joseph C. Panettieri, "Are Your Computers Safe?" Information Week, 28 Nov.94, 3.

37. Bob Berwin, "Naval Academy Network Stung by Hacker Attack," Federal Computer Week, 9.2, 23 Jan. 95, 3.

38. Peter Schweizer, Friendly Spies, New York: Atlantic Monthly Press, 1993, 158.

39. Wayne Madsen, "Intelligence Agency Threats to Computer Security," International Journal of Intelligence and Counterintelligence, 6.4 (Winter 1993), 421.

40. Madsen, 418.

41. Alger, 6.

42. SAIC, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 2-68.

43. United States, Congress, Office of Technology Assessment, 2.

44. Madsen, 437-438.

45. Douglas Waller, "Onward Cyber Soldiers," Time, 21 Aug. 1995: 43.

46. Neal Pollard, Computer Terrorism," address, 1995 International Information Warfare Conference, Arlington VA, 7 Sep. 1995, 11.

47. Bob Hohler and Hiawatha Bray, "Computer Wiretap Helps Track Hacker," Boston Globe, 30 Mar. 1996: 1.

48. "Hacker Boasted of Access to US Computers, Newspaper Says," Boston Sunday Globe, 31 Mar. 1996: 23.

49. Madsen, 419.

50. Madsen, 422.

51. Madsen, 421.

52. United States, National Communications System, 2-5, 2-18.

53. Pollard, 6.

54. Pollard, 13.

Appendix B: The Day After...In Cyberspace

No.	Incident Description
1.	May 7 - Iran announces it would soon begin conducting military exercises "appropriate to the evolving security situation in the Gulf."
2.	May 10 - Tehran radio and TV announced that Iranian Foreign Minister was flying to Riyadh with an "urgent proposal" that would "resolve the OPEC stalemate" and "respond to the evolving security situation in the region."
3.	May 11 - 90% of the power in the Cairo area went out for several hours. Cause: unknown
4.	May 11 - The public switched network for Northern California and Oregon suffers a series of massive failures. Cause: trap door[a].
5.	May 11 - The base phone system in Fort Lewis, WA is subjected to a mass dialing attack by personal computers.
6.	May 13 - The largest ARAMCO refinery near Dhahran has a catastrophic flow control malfunction which leads to a large explosion and fire.
7.	May 14 - Iran sends messages to Gulf Coordinating Council members, the US, the UK and France calling for negotiations. Messages sent to the Kuwait and Saudi leaders state Iran will soon "demonstrate the futility of depending upon the American imperialists for protection from modern weapons systems."
8.	May 14 - A new, high-speed Metro-Superliner traveling at 300 km/hr slams into an apparently misrouted freight train near Laurel, MD. The wreck kills over 60 passengers and crew and injures another 120. Cause: logic bomb.[b]

---

[a] "A hidden software mechanism triggered to circumvent system security measures. This can be a legitimate programming technique that allows a developer to bypass lengthy log-on routines or access source code directly. Its existence, if known by unauthorized persons, however, can be the source of a significant security breach." Definitions for the Discipline of Information Warfare and Strategy, Washington: School of Information Warfare and Strategy, National Defense University, Jul. 1995), 79.

[b] "A type of Trojan horse that may or may not be a virus. Its mission component is triggered by a true/false condition. Logic bombs do not propagate; they just sit and wait." A Trojan horse is a "malicious computer code that is located within a desirable block of code, (i.e., an application program, operating system software, etc.). To be a Trojan horse, the presence of the code must be unknown and it must perform an act that is not expected by the owner of the system," Definitions, 46 and 80.

9. May 15 - The Iranian Ambassador to the UN is overheard to state that as US is "the technologically most advanced power on the planet," it is highly vulnerable to "21st Century attacks" by "states and others who had mastered contemporary computer and telecommunication technology."

10. May 16 - Scotland Yard informs the Prime Minister that the Bank of England had detected "three different sniffer devices[c] of a new design in its main funds transfer system" and bank officials were fearful that unauthorized individuals could now enter the funds transfer system.

11. May 16 - CNN airs a "Special Report" which features the Metroliner train wreck and leaked reports about the Bank of England. CNN states "some Western intelligence agencies" believe that Iran may be employing computer experts from the Russian Mafiya and "renegade software writers" from India to "threaten the entire economic fabric of the United States and West Europe." Thereafter, the London Stock Exchange Index falls 10% and the New York Stock Exchange suffers its largest drop since the crash of 1987. Business news networks speculate the losses are caused by major institutional investors attempting to get out of the electronically managed market. The Security and Exchange Commission reports a pattern of institutional investment manipulation involving unknown parties working through European and Middle Eastern Banks.

12. May 17 - The Consortium for Planetary Peace (CPP) announces that an "emergency mobilization to stop an unnecessary and potentially devastating war" will take place in 48 hours. Two hours later, it files a request for a permit for the Mall with the US Park Police to accommodate and estimated 100,000 participants.

13. May 20 - The Senate in the face of an aggressive lobby campaign by CPP passes a resolution supporting the President's decision to send troops to the Gulf by two votes.

14. May 20 - DoD discovers there is corrupt data in the Time Phased Force Deployment List (TPFDL).

15. May 20 - The automatic tellers of the two largest bank chains in Georgia start to malfunction with bank clients being debited and/or credited thousands of dollars after each ATM transaction. By midday, they shut down their ATM machines.

---

[c] Software programs designed to analyze a communications network. They diagnose problems and assist network administrators in fixing them. In some cases, the software is written so that network administrators are unaware someone else is snooping through the networks collecting information, such as passwords, tapping databases, and listening in on telecommunications transmissions. Sniffers may be written to ferret out information which will permit the user to surrepetiously enter and/or manipulate the system later on. Schwartau, 116.

16. May 20 - CNN airs a "Special Report" focused on the vulnerability of the US to "cyberspace warfare" - dwelling on the Metroliner crash, the telephone outage in the Northwest, the ATM malfunctions and the interference with CNN's own transmissions. Interviews accompanying the program convey a growing sense of public concern that the US was far more vulnerable to IW attack than "the government has told us."

17. May 21 - The Russian Foreign Minister criticizes the US and allied deployments to the Gulf as "dangerous brinkmanship" and offers to host an international summit to defuse the crisis.

18. May 21 - The CPP "anti-intervention" demonstration in Washington far exceeds expectations and draws 400,000 people.

19. May 22 - The pilot of a new Continental Airlines AB-340 jet making a final approach to O'Hare International Airport reports his flight deck avionics has suffered a massive malfunction and that the aircraft is out of control. It crashes killing 30 and injuring another 100. A report concludes the AB-340 and 330 flight control software may be infected by a sophisticated logic bomb and the FAA grounds all such aircraft.

20. May 23 - The news anchors of the Saudi Government's networks were suddenly replaced by the face of the head of the CIRD Council who called on the citizens of Saudi Arabia "to join forces in the peaceful transformation of the Saudi kingdom to freedom and democracy under Islam." The pre-arranged signal leads to large scale demonstrations against the Saudi monarchy.

21. May 23 - The Saudi public switched network begins to fail apparently due to unauthorized modification of the system through a trap door.

22. May 23 - The local television station in Dhahran announces that the "Provisional Islamic Republic of Arabia" had seized power in Dhahran and Mecca. He states that Iranian military assistance "would be immediately halted if foreign nations let the Arabian revolution proceed on its own."

23. May 23 - The Secretary of Defense is informed that a full scale IW attack of unknown sources is underway at "almost every military base in the United States and Europe" involved in the deployment to Saudi Arabia.

24. May 24 - At a news conference held at the CNN news room, the CPP denounces the "criminal action which led to the Airbus tragedy at O'Hare" but concluded that "legitimate protest should not be quashed by the terrorist acts of a few." It announces it was "mobilizing all of its chapters to conduct civil disobedience

actions to stop the US Government's mad dash to war to save an undemocratic and failed Saudi regime."

25. May 24 - Several JSTARS aircraft operating in the Gulf region appear to be plagued with a computer worm[d] triggered by some external source.

26. May 24 - The entire phone network in the Washington/Baltimore region including local cellular systems fails. A preliminary assessment suggests an attack through a trap door has caused it.

27. May 24 - The Chicago Commodity Exchange experiences some of its "wildest fluctuations in history." There is widespread suspicion that "the Exchange was being subjected to a powerful form of electronic manipulation by parties unknown."

28. May 24 - CBS Evening News was interrupted for seven minutes by the "Action Arm of the Committee for Planetary Peace." During the video take over, the CPP spokesperson, a well known and highly regarded media personality, called for widespread civil disobedience to thwart an Administration which has "lost touch with domestic and international reality."

Incident Number	Type of Attack	Wpns Cat	Tgt Ctr of Gravity
1. Iranian Exercises	Persuasion	Perc Mgmt	Leaders
2. Iranian Diplomatic Initiative	Persuasion	Perc Mgmt	Leaders
3. Cairo Power Outage	Logic Bomb	Corruption	System Essential
4. CA and OR PSN Shutdown	Trap Door	Corruption	System Essential
5. Ft Lewis mass dialing attack	Info Overload	Corruption	Defense Mechanism
6. ARAMCO Explosion	Logic Bomb	Corruption	System Essentials
7. Iran Message to GCC	Persuasion	Perc Mgmt	Leaders
8. Metroliner Crash	Logic Bomb	Corruption	Infrastructure
9. Iranian Ambassador Statement	Discourse	Perc Mgmt	Leaders
10. Bank of England	Sniffers	Corruption	System Essentials
11. CNN "Financial Targets" Report	Persuasion	Perc Mgmt	Population
12. CPP Press Release	Slogans	Perc Mgmt	Population
13. Close Vote in Senate	Argument	Perc Mgmt	Leaders
14. TPFDL Pollution	Virus	Corruption	Defense Mechanism

[d] A computer program that eats up the memory and resources of a computer, effectively rendering it useless. Schwartau, 120.

15. Bank ATMs malfunction	Logic Bomb	Corruption	System Essentials
16. CNN Govt Coverup Report	Persuasion	Perc Mgmt	Population
17. Russian Diplomatic Initiative	Persuasion	Perc Mgmt	Leaders
18. CPP Demonstration	Slogans	Perc Mgmt	Leaders
19. Airplane Crash	Logic Bomb	Corruption	Infrastructure
20. Saudi News Takeover	Spamming	Perc Mgmt	Population
21. Saudi PSN Shutdown	Logic Bomb	Corruption	System Essentials
22. Saudi TV Announces Coup	Misinformation	Perc Mgmt	Population
23. IW Attacks Against US Bases	Multiple Efforts	Corruption	Defense Mechanism
24. CPP News Conference	Argument	Perc Mgmt	Population
25. JSTARS Malfunction	Worm	Corruption	Defense Mechanism
26. D.C./Balt Phone Shutdown	Logic Bomb	Corruption	System Essentials
27. Chicago Exchange Fluctuations	Logic Bomb	Corruption	System Essentials
28. CBS News Takeover	Spoofing	Perc Mgmt	Population

(Fig. B-1) Illustrative incidents from RAND wargame "The Day After...in Cyberspace"

TOTALS:

WEAPON TYPES

Destruction - 0
Corruption - 14
Perc Mgmt - 14

CENTERS OF GRAVITY TARGETED

Leaders - 7
System Essentials - 8
Infrastructure - 2
Population - 7
Defense Mech - 4

The capabilities required to produce the incidents used in the RAND "Day After" exercise have, for the most part, already been seen. Figure B-2 attempts to provide examples of similar world events for each technology related incident in the wargame.

The assumption of the exercise is that a malevolent actor intentionally assembles these capabilities in a structured attack. The Kevin Poulsen details, provided in item 21, show some blending of capacity and intent. Individual account descriptions are provided below.

Incident Number	Type of Attack	Similar World Event
3. Cairo Power Outage	Logic Bomb	Computer Espionage
4. CA and OR PSN Shutdown	Trap Door	LOD Time Bomb
5. Ft Lewis mass dialing attack	Info Overload	Noted Intruder Skills
6. ARAMCO Explosion	Logic Bomb	Kevin Poulsen Pleas Guilty
8. Metroliner Crash	Logic Bomb	1995 Arizona Railway Incident
10. Bank of England	Sniffers	Citibank $10 million Fraud Case
14. TPFDL Pollution	Virus	Paid Informants
15. Bank ATMs malfunction	Logic Bomb	$70 Million Software Glitch
19. Airplane Crash	Logic Bomb	Disgruntled Def. Contractor Emp.
20. Saudi News Takeover	Spamming	Demonstrated Technology
21. Saudi PSN Shutdown	Logic Bomb	Kevin Poulsen Pleas Guilty
23. IW Attacks Against US Bases	Multiple Efforts	DISA Red Team Results
25. JSTARS Malfunction	Worm	Electronic Intruders
26. D.C./Balt Phone Shutdown	Logic Bomb	Other Phone System Failures
27. Chicago Exchange Fluctuations	Logic Bomb	Shutdown Options
28. CBS News Takeover	Spoofing	Demonstrated Technology

(Fig. B-2) RAND Wargame Incident Comparison

REAL WORLD SIMILAR ACCOUNT DESCRIPTIONS

3. Computer Espionage - German intelligence agents managed to illegally access hundreds of computers worldwide through NASA's SPAN network. They managed to break into the CERN physics laboratory computer system in Geneva and loaded a damaging Trojan Horse that destroyed software and crashed systems.[1]

4. Legion of Doom's (LOD) PSN Time Bombs - In 1990, several Atlanta branch LOD members were arrested on charges of penetrating and disrupting telecommunication network elements. Federal agents accused the LOD members of planting a series of destructive "time bomb" programs in network elements in Denver, Atlanta, and New Jersey. These time bombs were designed to shut down major switching hubs, but were defused by telephone company employees before they caused damage. "Based on an analysis of open source literature, the author believes that groups of electronic intruders, if organized and funded by interested adversaries, have the capabilities to launch sophisticated widespread attacks on and across the PSN. These types of attacks could result in significant degradations in the nation's NS/EP telecommunication capabilities, create significant public health and safety problems, and cause serious economic shocks."[2]

5. Noted Intruder Skills - Electronic intruders have shown the abilities to service control points,

service provisioning systems, cross-connect systems, modify user services, forward calls, modify service class on circuit, turn off billing on specific circuits, routing tables, and service descriptions. Scott Maverick compromised 911 services in 1992. He was arrested for tampering with these systems in Virginia, Maryland, and New Jersey. Maverick said his intent was to infect the 911 computer with a virus to cause havoc. "Significant degradation of service for 911 systems is possible if they are targeted by electronic intruders."[3]

6. Kevin Poulsen Pleas Guilty - Allegedly masterminded an April 1991 effort for a complete computer and telephone system invasion. The most comprehensive, coordinated attack on the PSN to date. Pleaded guilty to all but one of the following counts: compromised an ongoing law enforcement investigation; identified law enforcement run businesses and law enforcement wiretaps; intruded on Local Exchange Carrier (LEC) service provisioning system numerous times (allegedly more than 40); modified existing telephone services, added new telephone services (some without billing), forwarded calls to other numbers, and dual-provisioned telephone lines; intruded on LEC maintenance/test systems to electronically monitor telephone conversations; intruded on LEC databases and obtained telephone numbers (some unlisted), street addresses, customer names, and other sensitive data; physically broke into carrier offices, and stole equipment, software, identification badges, and other material; sold sensitive data obtained from LEC databases, and illegally established or modified telephone services for other individuals; manufactured false identification, including telephone company identification badges and drivers licenses; intruded on other computer systems for profit, including the California DMV, credit bureaus, and an Air Force computer network; illegally possessed classified documents (the one count he pleads not guilty on); laundered money. Although Poulsen did not attack PSN networks, he manipulated the system to his own ends and to his own personal profit.[4]

8. Arizona Railway Incident - Investigation of the 1995 crash in an isolated portion of Arizona desert revealed a computer monitored safety device had been short-circuited. The system was supposed to warn of sequential loose rails but failed to operate because of apparently intentional tampering.

10. Citibank $10 Million Fraud Case - A 34 year old Russian, operating from St Petersburg, managed to gain access codes and move $10 million in funds from Citibank accounts in Argentina and Indonesia. Combine this capability with a 1994 case at a California university where an unauthorized program collected tens of thousands of account names and passwords through a "sniffer" program on the internet before it was found.[5]

14. Paid Informants - NCS says there is significant evidence of insiders selling information to information brokers, industrial spies, criminal organizations, and intelligence services. These insiders, with full access to their respective information files, have provided data on unpublished telephone numbers, toll records, credit reports, and other personal data. The FBI reported that criminal organizations have gained access to the National Crime Information Center records primarily through the use of compromised employees. In December 1991, 18 Social Security Administration employees were indicted for sale of confidential information.[6]

15. $70 Million Software Glitch - A $70 million government loss due to overpayment by the Health Care Financing Administration was caused by a software problem which failed to crosscheck Medicaid eligible people against Medicaid claims. The money was spent for services provided, however, not all patients were eligible. The largest organization overpayment was $19,000,000.[7]

19. Disgruntled Defense Contractor Employee - In August 1992, a computer systems administrator for a defense contractor was told of a pending layoff. The employee set up a malicious code to activate after his departure. He hoped that the company would hire him back to reconstruct databases after the logic bomb functioned. His attempt was discovered before he left and he later pleaded guilty to the charge. If the malicious code had functioned, substantial data on the development of military missile systems would have been destroyed and required months to reprogram the computer system.[8]

21. See item six.

23. DISA Red Team Results - The team attempted to gain access to 9,000 computers across the defense department. They successfully hacked into 88%, over 7,900, of the computers. They left signs of their trespass yet only just over 300 of the illegal entries were detected. Network administrators at the Air Force Information Warfare Center said they could crack 70% of the passwords on their UNIX network with tools resembling those now being used by Internet hackers.[9]

25. Electronic Intruders - There is growing evidence of the use of electronic intrusion techniques by industrial spies. In a survey of 150 high technology research and development companies, 48 percent said they had been the target of trade secret theft. Combine this information with the case of Kevin Mitnick. He was arrested and prosecuted in 1989 for stealing more than $1 million in source code from Digital Equipment Corporation (DEC), modifying it to add "trap doors," and attempting to copy it back to DEC's development computers.[10] JSTARS is highly software dependent program that could be vulnerable to this type of intrusion.

26. Other Phone System Failures - A 1991 near total shutdown of telephone service in the Baltimore-Washington area was caused by a coding error in new ATT long-distance software. A highway crew digging post holes disrupted coast to coast calls by cutting a MCI fiber-optic cable. A similar incident in New Jersey cut 60% of the calls in and out of Manhattan for eight hours. In this incident the New York Mercantile Exchange and the Commodity Exchange had to shut down operations. Additionally, voice and radar systems used to control air traffic from facilities in New York, Washington, and Boston were disabled for five hours.[11]

27. See item 26 and other cases of software manipulation.

	Leaders	System Ess	Infrastructure	Population	Def Mech
Destruction Physical Destruction					
Corruption Internal Operating Logic		**3 Cairo Pwr 4 CA/OR PSNs 6 ARAMCO 10 Bank of Eng 15 ATMs 21 Saudi PSNs 26 DC/Bal PSN 27 Chicago Trd**	**8 Metroliner 19 Airplane**		**5 Ft Lewis 14 TPFDL 23 IW Attks 25 JSTARS**
Perception Management Behavior	**1 Iran Exercise 2 Iran Dipl Init 7 Iran Msg 9 Iran Ambass 13 Senate Vote 17 Russia Dipl 18 CPP Demo**			**11 CNN Rpt 12 CPP Pr Rel 16 CNN Rpt 20 Saudi News 22 Saudi Coup 24 CPP News 28 CBS News**	
Ignore					

(Fig. B-3) Illustrative information incidents placed in framework.

	Leaders	System Ess	Infrastructure	Population	Def Mech
Destruction Physical Destruction		6 ARAMCO	8 Metroliner 19 Airplane	8 Metroliner 19 Airplane	
Corruption Internal Operating Logic		3 Cairo Pwr 4 CA/OR PSNs 5 Ft Lewis 6 ARAMCO 10 Bank of Eng 15 ATMs 21 Saudi PSNs 23 IW Attks 26 DC/Bal PSN 27 Chicago Trd	8 Metroliner 19 Airplane	3 Cairo Pwr 4 CA/OR PSNs 15 ATMs 21 Saudi PSNs 26 DC/Bal PSN 27 Chicago Trd	5 Ft Lewis 14 TPFDL 23 IW Attks 25 JSTARS
Perception Management Behavior	1 Iran Exercise 2 Iran Dipl Init 3 Cairo Pwr 4 CA/OR PSNs 5 Ft Lewis 6 ARAMCO 7 Iran Msg 8 Metroliner 9 Iran Ambass 10 Bank of Eng 11 CNN Rpt 12 CPP Pr Rel 13 Senate Vote 14 TPFDL 15 ATMs 16 CNN Rpt 17 Russia Dipl 18 CPP Demo 19 Airplane 20 Saudi News 21 Saudi PSNs 22 Saudi Coup 23 IW Attks 24 CPP News 26 DC/Bal PSN 27 Chicago Trd 28 CBS News			8 Metroliner 10 Bank of Eng 11 CNN Rpt 12 CPP Pr Rel 15 ATMs 16 CNN Rpt 19 Airplane 20 Saudi News 21 Saudi PSNs 22 Saudi Coup 24 CPP News 26 DC/Bal PSN 27 Chicago Trd 28 CBS News	5 Ft Lewis 14 TPFDL 23 IW Attks 25 JSTARS
Ignore					

(Fig. B-4) Using the framework to identify where the effects of information weapons fall.

1. Madsen, 421.
2. United States, National Communications System, 2-5, 4-2.
3. United States, National Communications System, 4-3, 4-5.
4. United States, National Communications System, 2-9, 2-10.
5. United States, National Communications System, 3-4; Hansell, 31.
6. United States, National Communications System, 2-13, 2-14.

7. SAIC, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, B-96.

8. United States, National Communications System, 2-13.

9. SAIC, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, B-66, B-72.

10. United States, National Communications System, 2-5, 2-18.

11. SAIC, Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance, 36; United States, GAO, 36.

Works Consulted

Adams, James. "The Role of the Media." Lecture. Information Warfare Course, National Defense University, Washington. 17 Dec. 1995.

Alberts, David S. Defensive Information War: Problem Formulation and Solution Approach. Washington: National Defense University, 17 Jan. 1996 5.

Alger, John. "Information Warfare: Hackers, Crackers and the Projection of Power." Address. 1995 - 1996 Third Tuesday Seminar Series: Interdisciplinary Aspects of the Electronic Superhighway. George Washington University, Washington. 17 Oct. 1995.

Allard, Kenneth C. "The Future of Command and Control: Toward a Paradigm of Information Warfare." Turning Point: The Gulf War and US Military Strategy. Ed. L. Benjamin Ederington and Michael J. Mazaar. Boulder: Westview Press, 1994 161-192.

Arquila, John and David Ronfeldt. "Cyberwar is Coming!" Comparative Strategy 12 (April-Jun. 1993): 141-165.

Arquila, John. "Information, Power and Grand Strategy: In Athena's Camp." Paper, Catigny Conference. Wheaton, Il. Jul. 1995.

- - - . "Strategic Implications of Information Dominance." Strategic Review (Summer 1994): 24-30.

Barnett, Jeff. The Revolution in Military Affairs. Briefing Slides. Washington: Dept. of Defense, Office of Net Assessment, 1995.

Boyd, John R. "A Discourse in Winning and Losing." Brief. Maxwell AFB, AL: Air University Library. 1987.

Brewin, Bob. "Naval Academy Network Stung by Hacker Attack." Federal Computer Week 9.2 23 Jan. 95: 3.

Broder, David S. "Looking Ahead in '92." Boston Globe 6 Apr. 1994: 15.

Brown, Michael. "Information Warfare." Lecture. Information Warfare Course, National Defense University, Washington. 17 Dec. 1995.

- - - . "Information Warfare and the RMA." Seminar on Intelligence and Command and Control. Cambridge, MA: Center for Information Policy Research, Harvard University January, 1996 1-27.

Builder, Carl H. "Rethinking National Security and the Role of the Military." Unpublished article. Santa Monica: RAND Corporation, 6 Sept. 1995.

Center for Disease Control. Addressing Emerging Infectious Disease Threats: A Prevention Strategy for the United States. Atlanta: Center for Disease Control and Prevention, Apr. 1994.

Christopher, Warren, et al. American Hostages in Iran: The Conduct of a Crisis. New Haven: Yale University Press, 1985.

Clausewitz, Carl von. On War. Ed. and trans. Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976.

Cleveland, Harlan. The Knowledge Executive: Leadership in an Information Society. New York: Dutton, 1985.

Conley, Robert. "Information Warfare Some Thoughts." Unpublished paper, 1993.

Cooper, Jeffery. "Another View of Information Warfare: Conflict in the Information Age." Prepublication draft. Washington: SAIC, 30 Aug. 1995.

Cooper, Pat. "Organized Crime Hackers Jeopardize Security of U.S." Defense News 3 Oct. 1994: 18.

Definitions for the Discipline of Information Warfare and Strategy. Washington: School of Information Warfare and Strategy, National Defense University, Jul. 1995.

deGraffenreid, Kenneth E. and Michelle Van Cleave. "Information Assurance and the Future of the NCS." Draft. Fairfax, VA: National Security Research Inc., 12 May 1995, 5-6.

Dunn, Richard J., III. From Gettysburg to the Gulf and Beyond: Coping With Revolutionary Technological Change in Land Warfare. Washington: Institute for National Strategic Studies, 2 May 1995 3.

Edmunds, Albert. Interview. Defense News 16 Oct. 1995: 102.

Elmer-DeWitt, Philip. "The Kid Put Us Out of Action." Time 14 Nov. 1988: 76.

Fairfield, John S. "A Jointly Focused Vision." Armed Forces Journal Jan. 1996: 37.

Fogleman, Ronald R. and Sheila E. Widnall. Cornerstones of Information Warfare. Washington: HQ, USAF, 1995.

Fogleman, Ronald R. "Information Operations: The Fifth Dimension of Warfare." Address. Armed Forces Communications Electronics Association. Washington. 25 Apr. 1995.

Franks, Frederick M. Address. Association of United States Army Symposium. Orlando, FL. 8 Feb. 1994.

Garigue, R. "Information Warfare: Developing a Conceptual Framework." Draft. Ottawa: Office of the Assistant Deputy Minister, Defense Information Services, 23 Aug. 1995.

Gertz, Bill. "French Spooks Scare Firms." Washington Times, 9 Feb. 1992.

Grove, Ronald. "The Information Warfare Challenges of a National Infrastructure." Address. 1995 International Information Warfare Conference, INFOCON Symposium. Arlington, VA. 7 Sep. 1995.

Haas, Lawrence J. "NII Security: The Federal Role." Address. National Information Infrastructure Security Issues Forum. Washington. 14 Jun. 1995.

"Hacker Boasted of Access to US Computers, Newspaper Says." Boston Sunday Globe, 31 Mar. 1996: 23.

Hansell, Saul. "Citibank Fraud Raises Computer Security Questions." New York Times 19 Aug. 1995: 1, 31.

Hohler, Bob and Hiawatha Bray. "Computer Wiretap Helps Track Hacker." Boston Globe, 30 Mar. 1996: 1.

International Energy Agency. The International Energy Agency Natural Gas Security Study. Paris: Organization for Economic Cooperation and Development/International Energy Agency, 1995, 183.

Jenner, Christopher. Faxed memorandum to authors, 5 Mar. 1996.

Joint Security Commission. Redefining Security. Washington: Joint Security Commission, Feb. 1994 vi.

Libicki, Martin C. The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon. Washington: Institute for National Strategic Studies, National Defense University, 1994.

- - - . What is Information Warfare? Washington: Institute for National Strategic Studies, National Defense University, Aug. 1995.

Lucky, Robert. Silicon Dreams: Information, Man and Machine. New York: St Martin's Press, 1989.

Lykke, Arthur F. Lecture. Army War College, Carlisle Barracks, PA. Jul. 1995.

Madsen, Wayne. "Intelligence Agency Threats to Computer Security." International Journal of Intelligence and Counterintelligence, 6.4 (Winter 1993): 413-487.

Plate, Thomas and William Tuohy. "John Major; Even Under Fire, Britain's Prime Minister Holds His Own." Los Angeles Times, 20 Jun. 1993; M.3.

Mann, Edward. Thunder and Lightning: Desert Storm and the Airpower Debates. Montgomery AL: Air University Press, 1995.

Marshall, Andrew W. "RMA Update." Memorandum for the Record. 2 May 1994.

McCarthy, Shawn P. "Network Break-ins Reveal the Chinks in Systems Security." Government Computer News 8 Aug. 1994: 63.

McNulty, Thomas J. "Television's Impact on Executive Decision Making and Diplomacy." Fletcher Forum on World Affairs 17 (Winter 1993): 81-82.

Molander, Roger C., Andrew S. Riddile, and Peter A. Wilson. "Strategic Information Warfare: A New Face of War." Draft. Santa Monica: RAND Corporation, 1995.

Morton, Oliver. "The Information Advantage." The Economist 10 Jun. 1995: 5.

Munro, Neil. "New Information Warfare Doctrine Poses Risks, Gains." Washington Technology 9.18 22 Dec. 1994: 1.

- - - . "The Pentagon's New Nightmare: An Electronic Pearl Harbor." Washington Post 16 July 1995 C3.

National Research Council. Computers at Risk: Safe Computing in the Information Age. Washington: National Academy Press, 1991.

National Research Council. Growing Vulnerability in Public Switched Networks: Implications for National Security Emergency Preparedness. Washington: National Academy Press, 1991.

National Security Telecommunications Advisory Committee (NSTAC). Report to NSTAC XVIII. Washington: National Information Infrastructure Task Force, Feb. 1996.

Neilson, Robert E. "The Role of Information Technology in National Security Policy." Acquisition Review Quarterly (Summer 1994): 192-201.

"Net Profit or Loss." Security Awareness News Oct. 1995: 8-10.

Panettieri, Joseph C. "Are Your Computers Safe?" Information Week 28 Nov. 1994: 3.

Pollard, Neal. "Computer Terrorism." Address. 1995 International Information Warfare Conference, Arlington VA. 7 Sep. 1995.

RAND Corporation. The Day After...in Cyberspace. Santa Monica: RAND, 1995.

RAND Corporation. Strategic Information Warfare: A New Face of War. Washington: RAND, 1995.

Ronfeldt, David. Cyberocracy, Cyberspace and Cyberology: Political Effects of the Information Revolution. Santa Monica: RAND, 1991.

Rosen, Stephen. Winning the Next War. Ithaca: Cornell University Press, 1994.

Ryan, Julie J. C. H. "Information Warfare: A Conceptual Framework." Lecture. Seminar on Intelligence and Command and Control. Center for Information Policy Research, Harvard University. Cambridge, MA. 7 Mar. 1996.

Sandberg, Jared. "GE Says Computers Linked to Internet Were Infiltrated." The Wall Street Journal, 28 Nov. 1994: B.5.

Schwartau, Winn. Information Warfare: Chaos on the Electronic Super Highway. New York: Thunder's Mouth Press, 1993.

Schweizer, Peter. Friendly Spies. New York: Atlantic Monthly Press, 1991.

Science Applications International Corporation. Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance. Washington: SAIC, 1995.

- - - . Planning Considerations for Defensive Information Warfare. Washington: SAIC, 16 Dec. 1993.

Sikorovsky, Elizabeth. "Internet Break-ins Compromise NASA Data." Federal Computer Week 19 Dec. 1994: 4.

Smith, James M. "Logic Flaw is the Culprit in Computer Mugging." Government Computer News 7 Nov. 1994: 12.

Soft Kill. CD-ROM. Xiphas, 1993.

Steele, Robert. "The Military Perspective on Information Warfare: Apocalypse Now." Address. Second International Conference on Information Warfare. Montreal. 19 Jan. 1995.

Stein, George. "Information Warfare." Airpower Journal (Spring 1995): 32.

Strassmann, Paul A. "Defending the Military Infrastructure." Address. Washington: National Defense University. 11 Mar. 1996.

- - - . "Risk-Free Access Into the Global Information Infrastructure Via Anonymous Re-Mailers," Symposium on the Global Information Infrastructure. Kennedy School of Government, Harvard University. Cambridge, MA. 28-30 Jan. 1996.

Summers, Harry G. On Strategy: A Critical Analysis of the Vietnam War. Novato, CA: Presidio Press, 1982.

Thompson, Mark. "If War Comes Home." Time 25 August 1995: 44-45.

Thurow, Lester. Head to Head: The Coming Economic Battle Among Japan, Europe and America. New York: Warner Books, 1993.

Toffler, Alvin and Heidi. War and Anti War: Making Sense of Today's Growing Chaos. New York: Warner Books, 1993.

United States. Air Force. The Nation's Air Force Booklet. Washington: HQ USAF, 1995.

- - - . Army. FM 100-5. Operations. Fort Monroe, VA: TRADOC, 1993.

- - - . - - - . "FM 100-6. Information Operations." Draft. Fort Monroe, VA: TRADOC, Jan. 1996.

- - - . - - - . Concept for Information Operations. Fort Monroe, VA: TRADOC, Aug, 1995.

- - - . Cong. House. Judiciary Committee. Hearings on the Threat of Foreign Economic Espionage to US Corporations. Washington: GPO, 29 Apr - 7 May 1992.

- - - . - - - . Office of Technology Assessment. Information Security and Privacy in Network Environments. Washington: GPO, Sep. 1994.

- - - . - - - . - - - . "Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage." Washington: GPO, Jun. 1990.

- - . - - - . Senate. Foreign Relations Committee. Hearings on the Subcommittee on Terrorism, Narcotics and International Operations. 103rd Cong., 2nd sess. Washington: GPO, 20-21 Apr. 1994.

- - - . Dept. of Defense. Joint Publication 3-0: Doctrine for Joint Operations. Washington: The Joint Staff, 1 Feb. 1995.

- - - . - - - . 1994 Defense Science Board Summer Study on Information Architecture for the Battlefield. Washington: Defense Science Board, 1994.

- - - . "Executive Order 12148, Federal Emergency Management." 44 Federal Register 43239. Washington: GPO, 20 Jul. 1979.

- - - . "Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions." 49 Federal Register 13471. Washington: GPO, 3 Apr. 1984.

- - - . "Executive Order 12656, Assignment of Emergency Preparedness Responsibilities." 53 Federal Register 226. Washington: GPO, 18 Nov. 1988.

- - - . "Executive Order 12919, National Defense Industrial Resources Preparedness" 59 Federal Register 29525. Washington: GPO, 3 Jun. 1994.

- - - . General Accounting Office. Information Superhighway: An Overview of Technology Challenges. Washington: GPO, 23 Jan. 1995.

- - - . National Communications System. An Assessment of Risk to the Security of Public Networks. Washington: National Communications System, Dec. 1995.

- - - . - - - . The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications: An Awareness Document. Washington: National Communications System, 1994.

- - - . Navy. Space and Electronic Warfare. Washington: GPO, 1992.

- - - . White House. National Security Strategy of the United States. Washington: GPO, August 1991.

Villacres, Edward J. and Bassford, Christopher. "Reclaiming the Clausewitzian Trinity." Parameters, Carlilse PA: US Army War College, Aug. 1995: 9-20.

Waller, Douglas. "Onward Cyber Soldiers." Time 21 Aug. 1995: 38-46.

Warden, John A., III. "The Enemy as a System." Airpower Journal (Spring 1995): 41-55.